

**СОДЕРЖАНИЕ**

[ВВЕДЕНИЕ 5](#_Toc171608504)

[АНАЛИТИЧЕСКАЯ ЧАСТЬ 8](#_Toc171608505)

[1 АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ 8](#_Toc171608506)

[1.1 Анализ подразделения ХХХХХХХХ организации ХХХХХ 8](#_Toc171608507)

[1.1.1 Дерево бизнес-направлений организации 8](#_Toc171608508)

[1.1.2 Сопоставление бизнес-процессов и критических факторов успеха системы менджмента информационной безопасности организации 9](#_Toc171608509)

[1.1.3 Анализ структуры и нормативной документации, регламентов подразделения «ххххххххххх» университета, регулирующих информационную безопасность 11](#_Toc171608510)

[1.2 Моделирование бизнес-процесса ххх хххххх ххххххх ххххххххххххххххх 12](#_Toc171608511)

[1.2.1 Моделирование ххххххххххххх “КАК ЕСТЬ” 12](#_Toc171608512)

[1.2.2 Моделирование процесса “КАК ДОЛЖНО БЫТЬ” 19](#_Toc171608513)

[1.3 Анализ рынка ПО для обеспечения информационной безопасности 22](#_Toc171608514)

[1.4 Анализ стейкхолдеров и их требований к разрабатываемой/модернизации СМИБ 23](#_Toc171608515)

[1.5 Определение области применения системы менеджмента информационной безопасности 23](#_Toc171608516)

[1.6 Выбор средств разработки/обеспечения ИБ 24](#_Toc171608517)

[1.7 Техническое задание на разработку корпоративной информационной системы 25](#_Toc171608518)

[1.8 Выводы по разделу 25](#_Toc171608519)

[ПРОЕКТНАЯ ЧАСТЬ 26](#_Toc171608520)

[2 ПРОЕКТИРОВАНИЕ И РАЗРАБОТКА ПРОЕКТА 26](#_Toc171608521)

[2.1 Структурирование требований к разрабатываемой системе 26](#_Toc171608522)

[2.1.1 Логическое моделирования данных 26](#_Toc171608523)

[2.1.2 Конструирование модели данных 28](#_Toc171608524)

[2.2 Разработка СМИБ 32](#_Toc171608525)

[2.2.1 Действия по обработке рисков и реализации возможностей 32](#_Toc171608526)

[2.2.2 Постановка задач (целей) в области информационной безопасности и планирование их достижения 45](#_Toc171608527)

[2.2.3 Корректирующие действия в случае выявления несоответствий СМИБ требованиям 46](#_Toc171608528)

[2.3 Разработка программной части для СМИБ 47](#_Toc171608529)

[2.3.1 План разработки ПО 47](#_Toc171608530)

[2.3.2 Frontend-разработка 47](#_Toc171608531)

[2.3.3 Backend-разработка 49](#_Toc171608532)

[2.3.4 Разработка модели доступа к данным 50](#_Toc171608533)

[2.3.5 Тестирование разработанного ПО 50](#_Toc171608534)

[2.4 План внедрения СМИБ (при необходимости добавить план развертывания ПО) 51](#_Toc171608535)

[2.5 Руководство администратора программной части СМИБ 52](#_Toc171608536)

[2.6 Документирование Политики информационной безопасности 53](#_Toc171608537)

[2.7 Выводы по главе 2 53](#_Toc171608538)

[ЭКОНОМИЧЕСКАЯ ЧАСТЬ 54](#_Toc171608539)

[3 ОБОСНОВАНИЕ ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ ОТ РАЗРАБОТКИ ИС 54](#_Toc171608540)

[3.1 Расчет затрат на разработку ИС 54](#_Toc171608541)

[3.2 Выбор и обоснование методики расчёта экономической эффективности 54](#_Toc171608542)

[3.3 Оценка затрат на разработку и внедрение АИС 54](#_Toc171608543)

[3.3.1 Затраты на этапе разработки информационной системы 57](#_Toc171608544)

[3.3.2 Затраты на этапе внедрения 59](#_Toc171608545)

[3.3.3 Затраты на этапе эксплуатации 60](#_Toc171608546)

[3.4 Эффект от внедрения АИС 60](#_Toc171608547)

[3.5 Экономический эффект 62](#_Toc171608548)

[3.6 Социальный эффект 64](#_Toc171608549)

[3.7 Научный эффект 64](#_Toc171608550)

[3.8 Организационный эффект 64](#_Toc171608551)

[3.9 Эффективность внедрения АИС (ПО ПРИМЕРУ) 65](#_Toc171608552)

[3.10 Расчёт показателей экономической эффективности проекта (ПО ПРИМЕРУ) 66](#_Toc171608553)

[3.11 Выводы по главе 3 74](#_Toc171608554)

[ЗАКЛЮЧЕНИЕ 76](#_Toc171608555)

[СПИСОК ЛИТЕРАТУРЫ 77](#_Toc171608556)

[ПРИЛОЖЕНИЯ 78](#_Toc171608557)

[Приложение 1. Техническое задание на разработку корпоративной электронной библиотеки в университете 78](#_Toc171608558)

[Приложение 2. Исходный код “Авторизация” 84](#_Toc171608559)

[Приложение 3. Руководство администратора корпоративной информационной системы 88](#_Toc171608560)

[Приложение 4. Политика информационной безопасности ЭТО ПРИМЕР! НЕ НУЖНО ВСЕ СЕБЕ КОПИРОВАТЬ!! 91](#_Toc171608561)

# ВВЕДЕНИЕ

В настоящее время в любой современной организации не зависимо от направления ее деятельности, внедрение информационных систем значительно упрощает управление деятельностью организации, оптимизирует внешние и внутренние процессы. Хххххх хххххх ххххххх хххххх ххх хх х ххххх ххххх хххххххххх хх ххххххх не каждый сотрудник того или иного отдела сможет решить более сложную техническую задачу в сфере IT. Потому, разработка информационной системы хххххх ххххххх хххххх ххххххххх ххххх ххххх ххх хххххххх, стала актуальной темой исследования. Для удобства использования, было принято решение разработать ИС на основе хххх хххххх ххххххх хххххх ххххххх ххххххх хххххх хххххх хххххх хххххххх ххххххх ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх.

**Актуальность работы** обусловлена ххххххх ххххххх ххххххх ххххххх ххххх.

**Объектом исследования** моей выпускной квалификационной работы стал хххххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх, в основную задачу которого, входит ххх хххххх ххххххх ххххххх ххххххх ххххххх хххххххх х ххххх ххххххх хххххх хххххх.

**Предметом исследования** выпускной квалификационной работы является ххххх хххххх хххххххх хххххх хххххххх ххххххх ххххххх хххххххх ххххххх ххххх хххх хххх ххххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх.

**Цель** выпускной квалификационной работы ххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх.

Основные задачи необходимые для достижения цели:

1. Провести анализ предметной области для выявления бизнес-процессов ххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх.
2. Сформировать необходимые функциональные требования к будущей ИС
3. Проанализировать базы данных (БД) и средства разработки для будущей ИС
4. Создать модель данных на физическом и логическом уровне.
5. Разработать ИС и создать диаграмму использования готового решения.
6. Оценить целесообразность разработки ИС и ее себестоимость.

Моя бакалаврская работа состоит из:

* Введения
* Первой главы - теоретическая часть
* Второй главы - практическая часть
* Третьей главы - экономическая часть
* Заключения - выводы
* Списка литературы

Первая глава, посвящена описанию структуры организации и ее деятельности, а так же ранее разработанному бизнес-процессу по приему заявок. Выявлены недостатки данного программного обеспечения и сформированы новые требования к разрабатываемой информационной системе.

Вторая глава, посвящена процессу разработки базы данных и самой информационной системы с диаграммой использования.

В третьей главе, описана экономическая часть проекта. Дана оценка себестоимости и целесообразности разработки данного продукта.

Ссылка на git-репозиторий с исходным программным кодом ХХХХХХХХХХХХХ

Ссылка на хостинг с размещенным веб-ресурсом ХХХХХХХХХХ

Учетные данные пользователя 1: логин ХХХХХХХХХХ пароль : ХХХХХХХХХХ

Учетные данные пользователя 2: логин ХХХХХХХХХХ пароль : ХХХХХХХХХХ

Учетные данные пользователя 3: логин ХХХХХХХХХХ пароль : ХХХХХХХХХХ

**При подготвоке ВКР заливку и красный текст убирать!**

# АНАЛИТИЧЕСКАЯ ЧАСТЬ

# АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ

## Анализ подразделения ХХХХХХХХ организации ХХХХХ

### Дерево бизнес-направлений организации

Построить дерево бизнес-направлений организации. Выделить в дереве **подразделение**, которое отвечает за выбранный вами бизнес-процесс.

Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх (рис. 1.1).

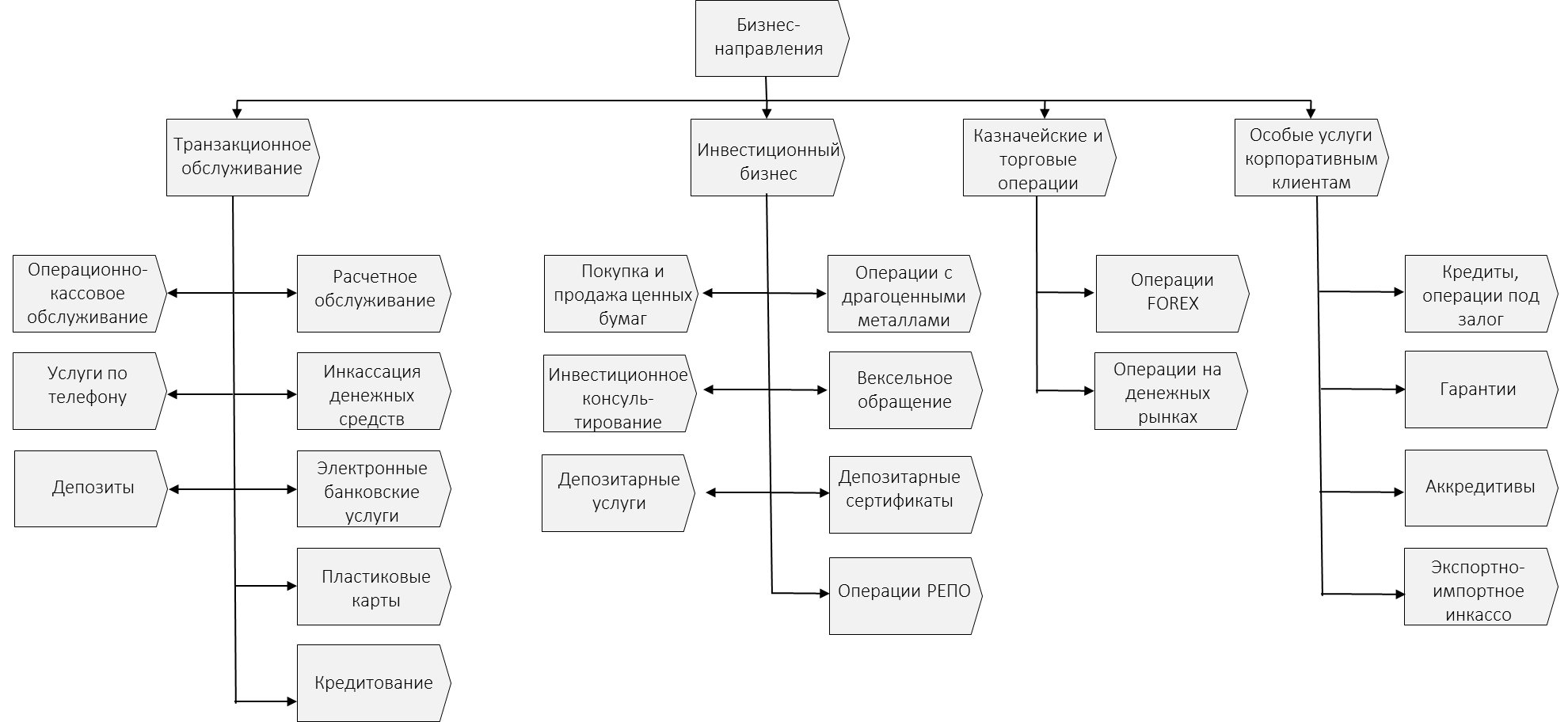


Рисунок 1.1 – Пример оформления рисунка

### Сопоставление бизнес-процессов и критических факторов успеха системы менджмента информационной безопасности организации

* Определить критические факторы успеха организации (самые важные стратегические цели компании)
* Сопоставить бизнес-процессы и критические факторы успеха
* Выбрать приоритетный бизнес-процесс, который в дальнейшем вы будете автоматизировать

Большое число факторов является критическими для успешного функционирования СМИБ, позволяющего организации достичь своих бизнес-целей. Примеры таких критических факторов успеха включают в себя:

a) политику и задачи в области информационной безопасности и действия, согласованные с этими задачами;

b) подход и общие принципы для проектирования, внедрения, мониторинга, обеспечения и улучшения информационной безопасности, согласованные с корпоративной культурой;

c) видимую поддержку и обязательства на всех уровнях управления, особенно на высшем уровне;

d) понимание требований по защите информационных активов, достигаемое применением менеджмента рисков информационной безопасности (см. ISO/IEC 27005);

e) действенное ознакомление с информационной безопасностью, подготовку и обучающую программу, информирующую всех сотрудников и другие соответствующие стороны об обязательствах в отношении информационной безопасности, которые сформулированы в политиках информационной безопасности, стандартах и т.д., а также их мотивирование поступать надлежащим образом;

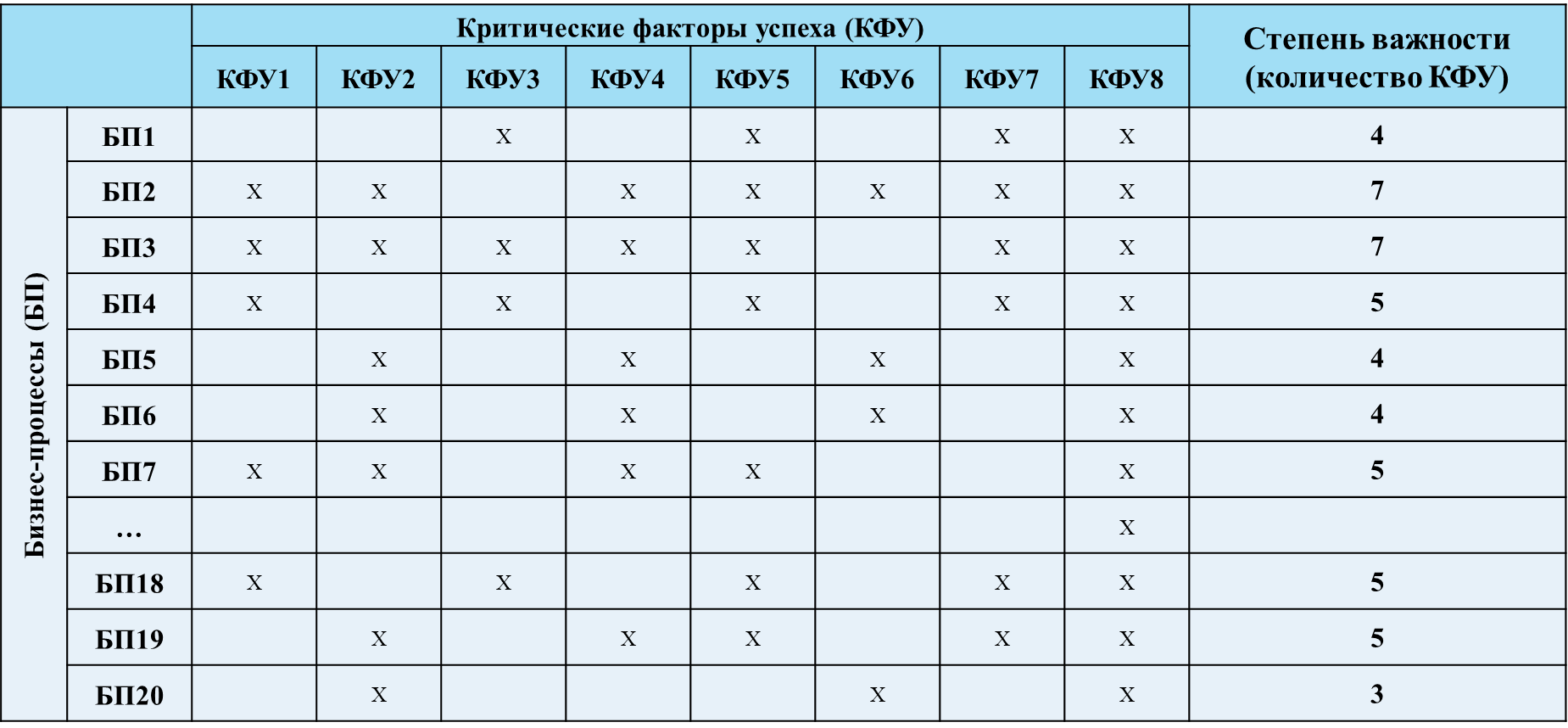
f) результативный процесс менеджмента инцидентами информационной безопасности;

g) действенный подход к менеджменту непрерывности бизнеса;

h) система измерений, используемая для оценки показателей деятельности в менеджменте информационной безопасности и предложения по улучшению, полученные по каналам обратной связи.

СМИБ увеличивает вероятность того, что организация будет постоянно обеспечивать критические факторы успеха, требуемые для защиты ее информационных активов.

Таблица . Матрица сопоставления бизнес-процессов и критических факторов успеха системы менджмента информационной безопасности



Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх.

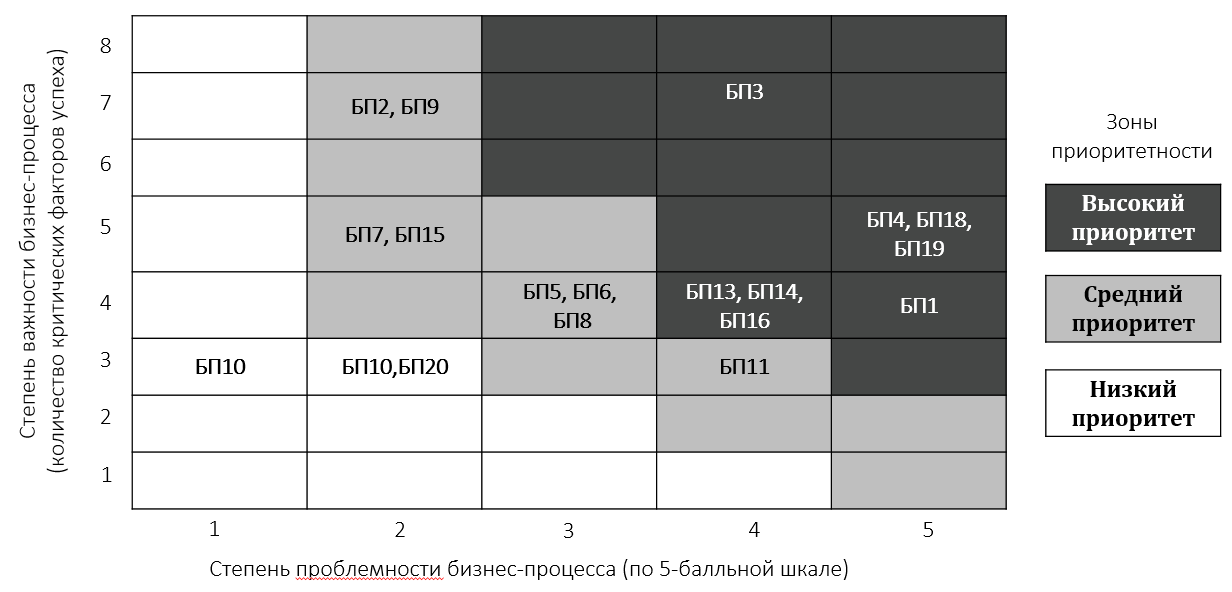


Рисунок 1.2 – Матрица ранжирования бизнес-процессов

### Анализ структуры и нормативной документации, регламентов подразделения «ххххххххххх» университета, регулирующих информационную безопасность

ВАЖНО! Здесь рассматривается именно подразделение, входящее в структуру организации. Например, не нужно рассматривать весь университет в целом, веберите один отдел и его анализируйте

Для вуза информацию можно взять на сайте МУИВ в разделе Сведения об образовательной организации

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх.

Этими задачами занимается отдел ххххх хххх ххххххххх.

В задачи которого входят:

1. ххххххх
2. хххххх
3. хххххххх
4. ххххххххх
5. хххххххх

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх.

## Моделирование бизнес-процесса ххх хххххх ххххххх ххххххххххххххххх

### Моделирование ххххххххххххх “КАК ЕСТЬ”

Бизнес-процесс **обязательно** должен быть представлен **ВО ВСЕХ** нотациях:

- IDEF0 (с декомпозицией)

- DFD (возможно использование нотации Гейна-Сарсона или Йордона-Де Марко)

- Диаграмма активностей (Activity diagram, диаграмма деятельности) в нотации UML, BPMN, EPC или IDEF3

Здесь же необходимо построить матрицу распределения ответственности

**Для каждой диаграммы/таблицы нужно сделать подробное описание!**

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх на рисунке 1.3.

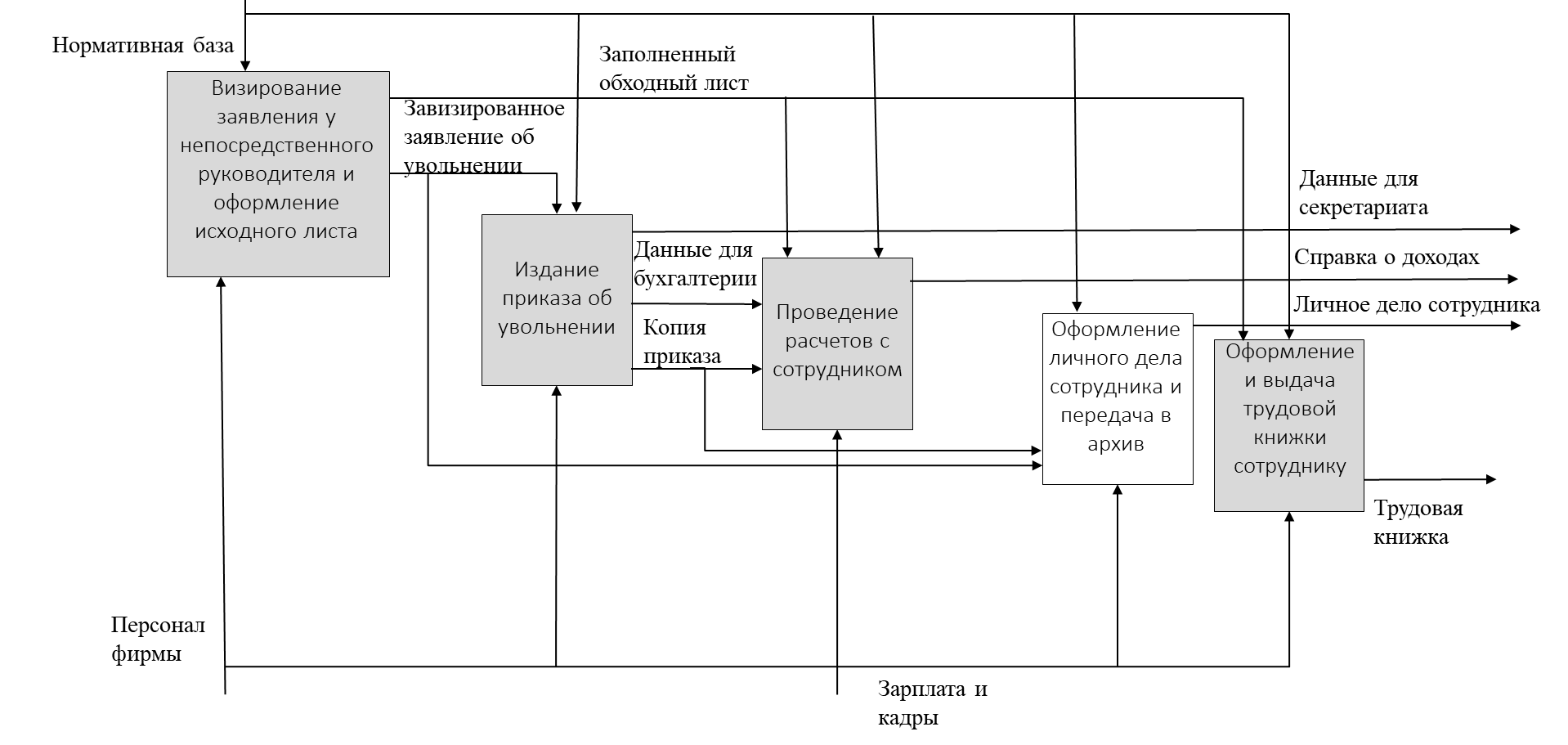


Рисунок 1.3 - IDEF0

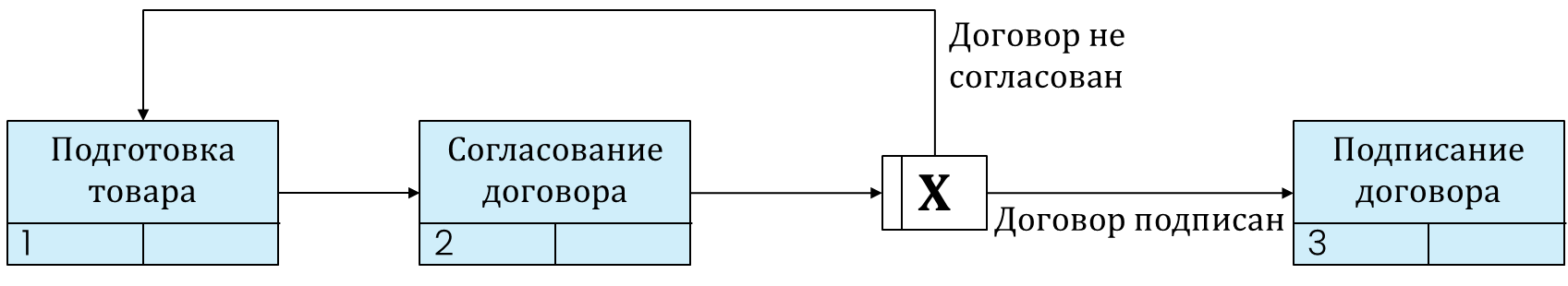


Рисунок 1.4 - IDEF3

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх.

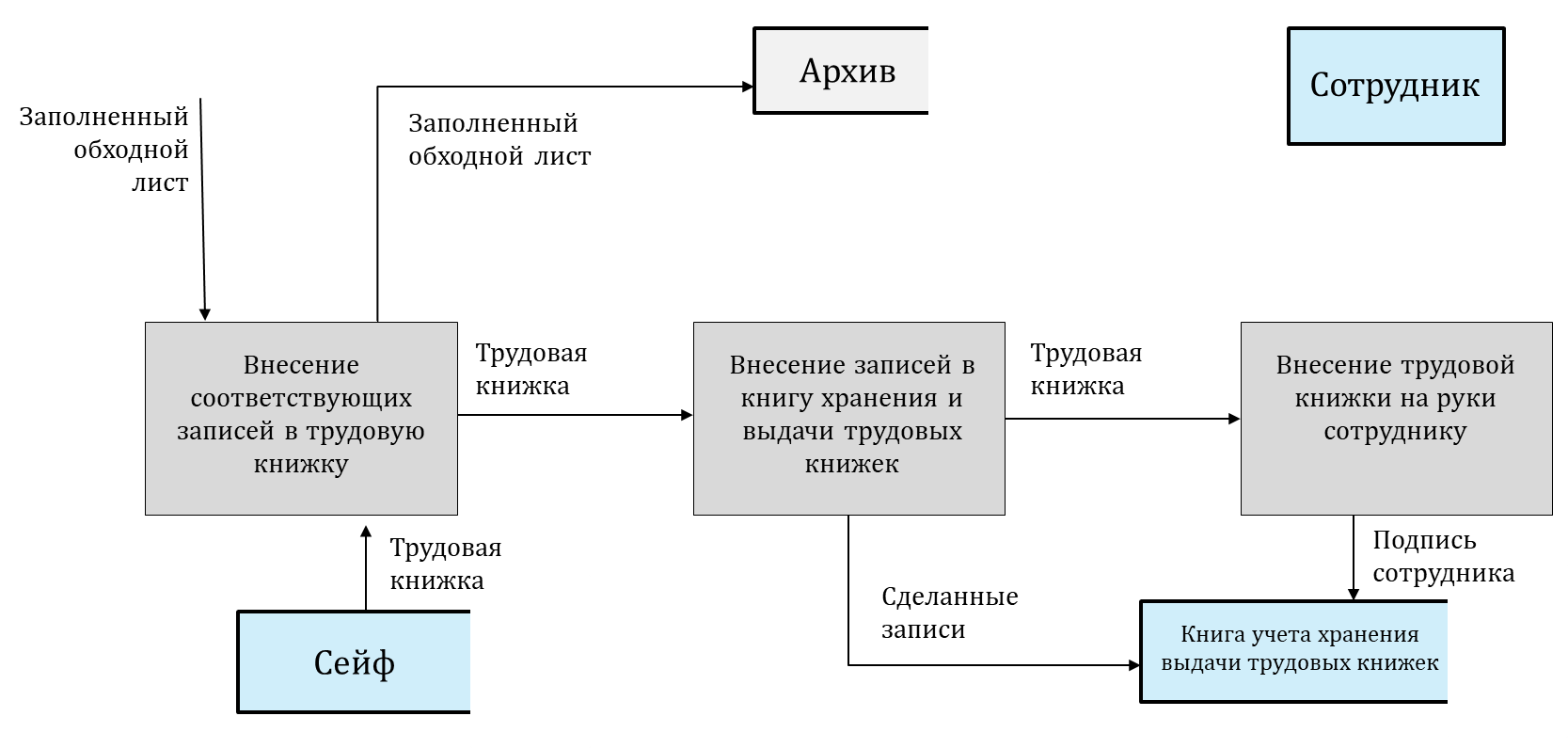


Рисунок 1.5 - Нотация Гейна-Сарсона (DFD)

На рисунке 1.5, изображена ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх.

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх.

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх на рисунке 1.6

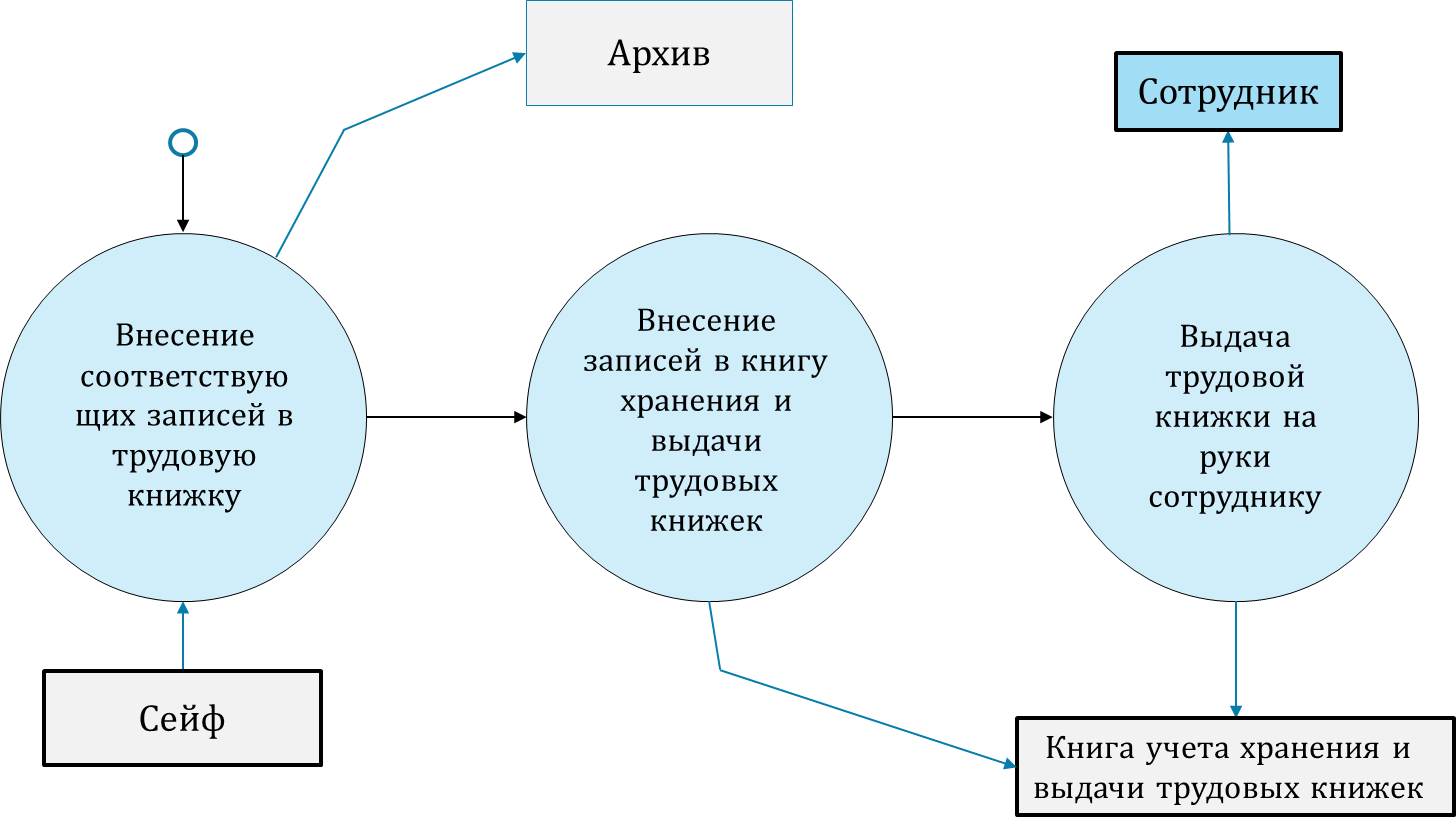


Рисунок 1.6 – Нотация Йордона-Де Марко (DFD)

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх.

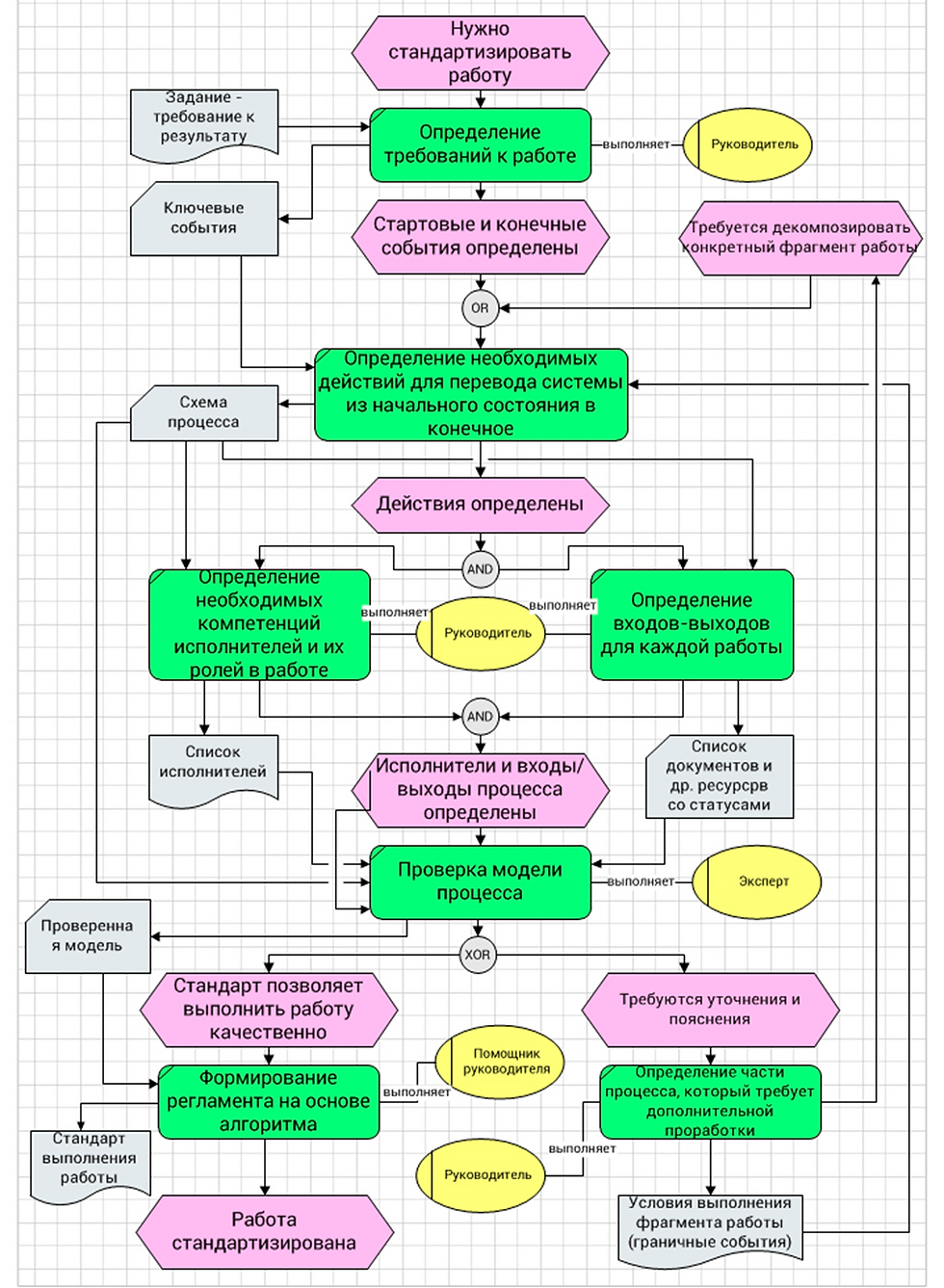


Рисунок Х.Х - Метод цепочки процессов, управляемой событиями (EPC)

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх.

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх.

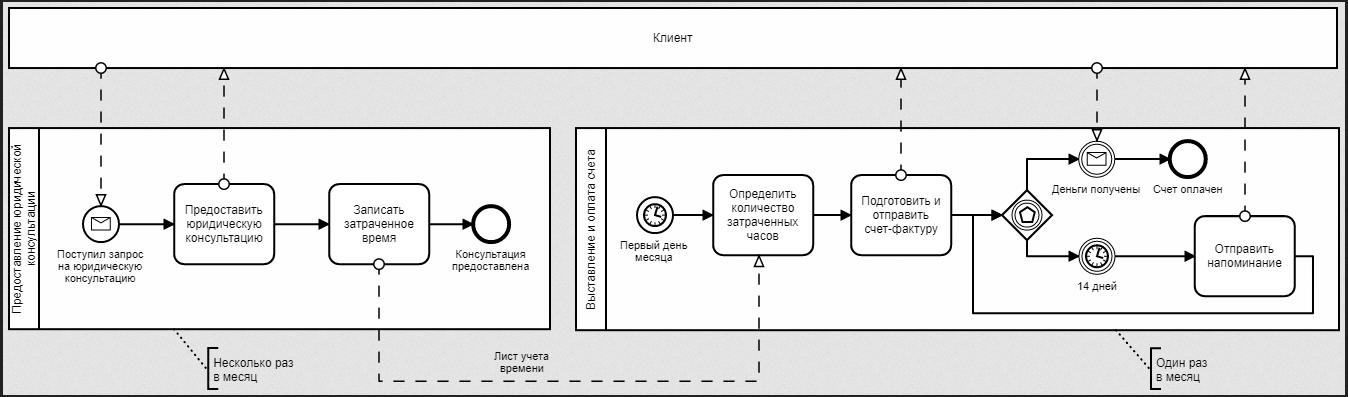


Рисунок Х.Х - Нотация BPMN

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх.

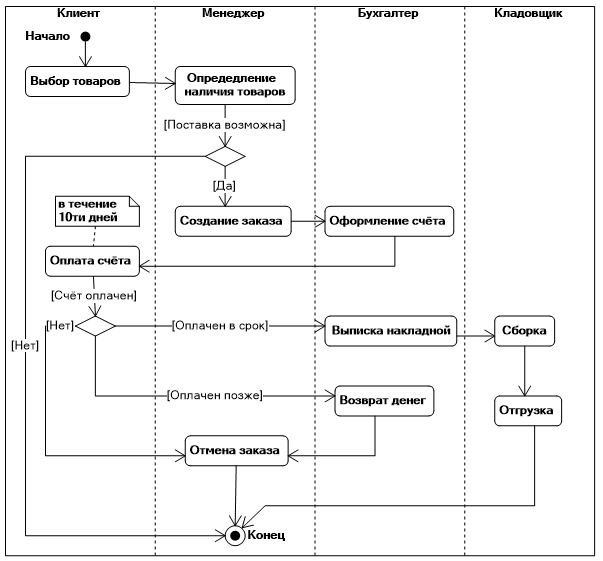


Рисунок Х.Х - Нотация UML - Диаграмма активностей (Activity diagram)

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх.

Таблица . Матрица распределения ответственности

|  |  |  |  |
| --- | --- | --- | --- |
|  | БП-1 | БП-2 | БП-3 |
| Отдел1 / Сотрудник1 | О | У | У |
| Отдел2/ Сотрудник2 | У | О | У |
| Отдел3/ Сотрудник3 | У | У | О |

\* О – ответственный за бизнес-процесс, У – участник бизнес-процесса

### Моделирование процесса “КАК ДОЛЖНО БЫТЬ”

Оценить степень проблемности бизнес-процесса

Разработать цели и ключевые показатели улучшения бизнес-процесса

Построить модель «КАК ДОЛЖНО БЫТЬ» **в той же нотации**, что и «КАК ЕСТЬ»

**Для каждой диаграммы/таблицы нужно сделать подробное описание!**

**Примечание**: К ключевым показателям относятся:

**Внешние**:

* Результаты бизнес-процесса
* Стоимость бизнес-процесса
* Длительность бизнес-процесса
* Качество результата бизнес-процесса (внешнее качество)

**Внутренние:**

* Качество выполнения бизнес-процесса (внутреннее качество)
* Организационная фрагментарность бизнес-процесса
* Информационная фрагментарность бизнес-процесса
* Количество выходов бизнес-процесса

**Примечание2**: Процесс в модели «КАК ДОЛЖНО БЫТЬ» должен быть оптимизирован (по сравнению с «КАК ЕСТЬ»)! Есть несколько методов оптимизации:

- метод минимизации устной информации и улучшения форм сбора и передачи информации

- метод параллельного выполнения бизнес-процессов

- метод устранения временных разрывов в бизнес-процессе

- метод разработки нескольких вариантов бизнес-процесса

- метод уменьшения количества входов и выходов бизнес-процесса

- метод согласования результатов процесса с требованиями клиентов

- метод интеграции процессов компании с процессами клиентов и поставщиков

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх.

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх.

Таблица . Шкала и критерии оценки БП и степени проблемности

|  |  |  |
| --- | --- | --- |
| **Оценка процесса** | **Критерии оценки** | **Значение степени проблемности** |
| Отлично | Потребители , аудиторы и владельцы считают, что выход процесса в значительной степени лишен недостатков. Нет также и операционных недостатков. Достигнуто серьезное улучшение в работе бизнес-процесса. Ожидается и планируется положительные изменения в будущем. | 1 |
| Хорошо | Было достигнуто хорошее улучшение показателей процесса по сравнению с планом. Ожидаются и планируются положительные изменения в будущем. | 2 |
| Удовлетворительно | Используемые в бизнес-процессе на данный момент процедуры является эффективными, нет серьезных проблем. Проводятся мероприятия по управлению процессом. Были разработаны ключевые показатели процесса. | 3 |
| Не очень хорошо | Бизнес-процесс обладает некоторыми операционными недостатками, которые требуют принятия мер для исправления. Недостатки можно исправить. Проводятся основные мероприятия по управлению процессом. | 4 |
| Плохо | Процесс неэффективен или почти не действует. Существуют серьезные недостатки, требующие принятия мер для исправления. Основные мероприятия по управлению процессом не проводятся. | 5 |

## Анализ рынка ПО для обеспечения информационной безопасности

Здесь должен быть обзор АНАЛОГОВ вашей системы.

**Не должно быть языков программирования и сред разработки! Для этого есть раздел 1.5!**

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх.

Таблица .

|  |  |  |
| --- | --- | --- |
| Название системы | Производитель | Стоимость годовой лицензии |
|  |  |  |
|  |  |  |
|  |  |  |

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх.

## Анализ стейкхолдеров и их требований к разрабатываемой/модернизации СМИБ

Выявить стейкхолдеров и их основые требования к разрабатываемой/модернизации СМИБ.

Определить:

a) заинтересованные стороны, которые значимы для системы менеджмента информационной безопасности;

b) значимые требования этих заинтересованных сторон;

c) какие из этих требований будут учитываться в системе менеджмента информационной безопасности.

ПРИМЕЧАНИЕ Требования заинтересованных сторон могут включать законодательные и нормативные требования и договорные обязательства.

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх.

## Определение области применения системы менеджмента информационной безопасности

Студент должен определить границы и сферу действия системы менеджмента информационной безопасности, чтобы установить ее область применения.

Определяя эту область, Студент должен принять во внимание:

a) внешние и внутренние факторы, указанные в разделе 4.1;

b) требования, указанные в разделе 4.2; и

c) взаимосвязи и зависимости между действиями, выполняемыми организацией, и теми, которые выполняются другими организациями.

Область действия должна быть оформлена как документированная информация.

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх.

## Выбор средств разработки/обеспечения ИБ

Здесь должен быть:

- краткий анализ существующего в организации ПО

- сравнительный анализ сред разработки, языков прогаммирования, СУБД, фреймворков

- выбор средств разработки для вашей системы

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх.

## Техническое задание на разработку корпоративной информационной системы

**ТЗ СТРОГО ПО ГОСТ 34.602-2020!!!! ТЗ выносится в приложение!**

Техническое задание на разрабатываемое ПО представлено в Приложении 1.

**ВАЖНО! Во всех заголовках, разделах, тексте название системы должно быть одинаково! Не должно быть в одном месте ИС, в другом АРМ, в третьем мобильное приложение**

## Выводы по разделу

В данной главе, рассмотрели структуру ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. На основании полученных данных было принято решение о целесообразности разработки проектируемой информационной системы для формирования / проверки / утверждения / и т.п. (в зависимости от поставленных задач) электронной библиотеки.

# ПРОЕКТНАЯ ЧАСТЬ

# ПРОЕКТИРОВАНИЕ И РАЗРАБОТКА ПРОЕКТА

## Структурирование требований к разрабатываемой системе

### Логическое моделирования данных

Разработать:

- UseCase диаграмму (нотация UML)

- Диаграмма последовательности (нотация UML)

- диаграмму функций

**Для каждой диаграммы/таблицы нужно сделать подробное описание!**

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх.

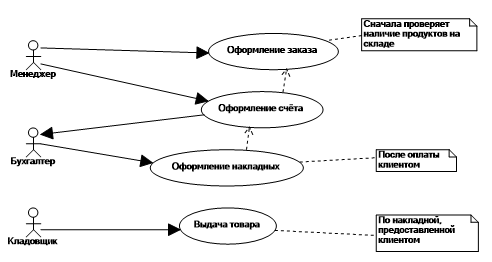


Рисунок Х.Х - Нотация UML - UseCase диаграмма (диаграмма вариантов использования)

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх.

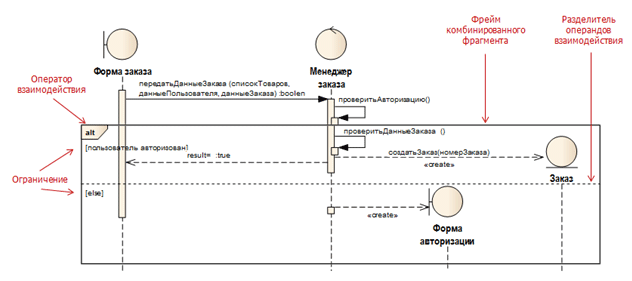


Рисунок Х.Х - Нотация UML - Диаграмма последовательности (Sequence diagram)

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх.

### Конструирование модели данных

Здесь разрабатывается база данных. Обязательны диаграммы «сущность-связь» (может быть оформлена в нотациях ER, IDEF1X, UML (Диаграмма классов (Class diagram)

Дополнительно может быть использована UML Диаграмма состояний (Statechart diagram)

**Все сущности должны быть описаны в тексте!**

**Для каждой диаграммы/таблицы нужно сделать подробное описание!**

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх.

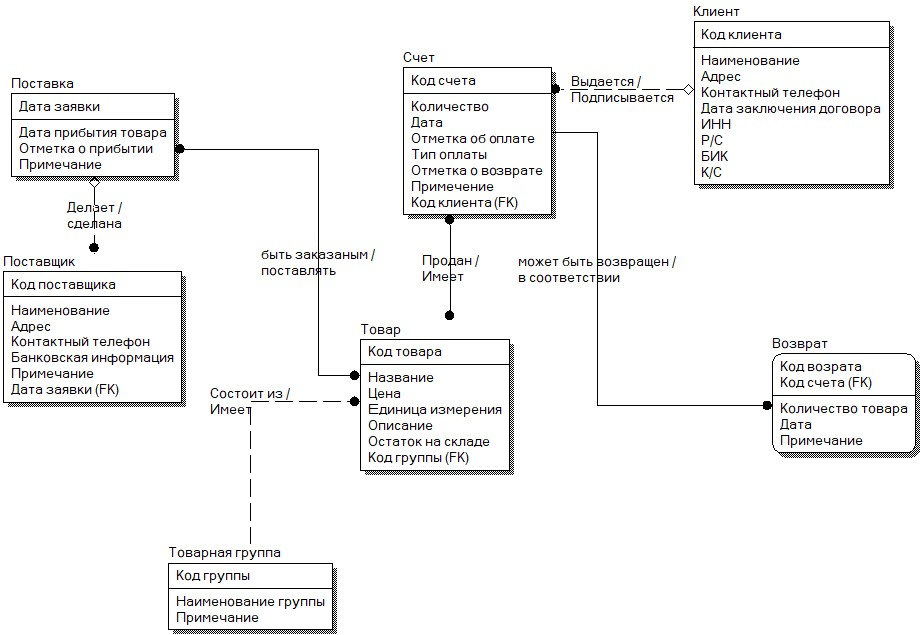


Рисунок Х.Х – ER-диаграмма (сущность-связь)

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх.

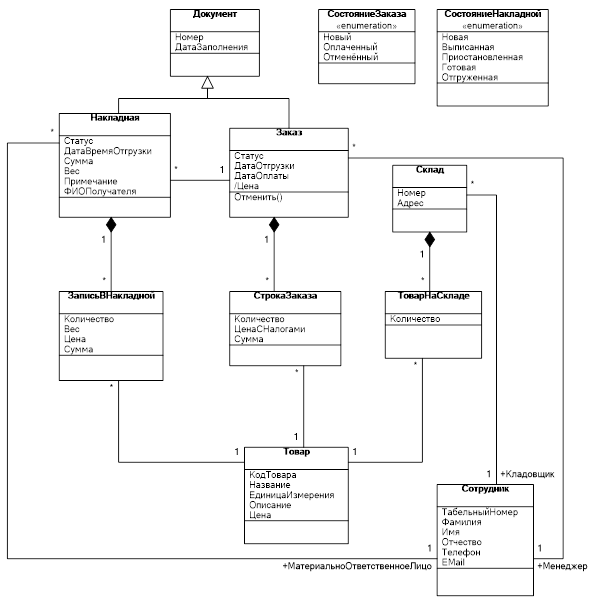


Рисунок Х.Х - Нотация UML - Диаграмма классов (Class diagram)

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх.

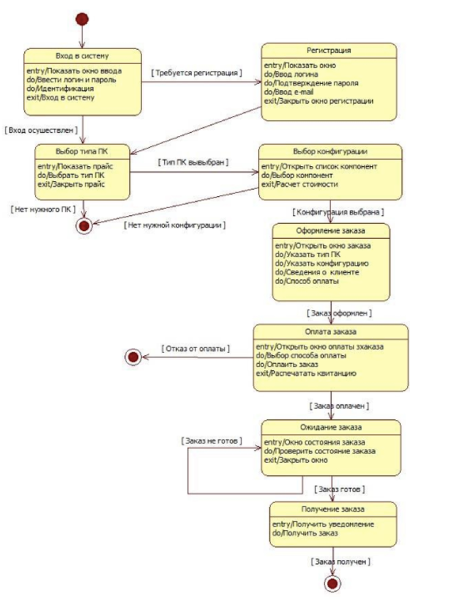


Рисунок Х.Х - Нотация UML - Диаграмма состояний (Statechart diagram)

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх.

## Разработка СМИБ

### Действия по обработке рисков и реализации возможностей

Планируя систему менеджмента информационной безопасности, Студент должен принять во внимание факторы, упомянутые в разделе 4.1, и требования, установленные в разделе 4.2, а также определить риски и возможности, в отношении которых должны быть предприняты действия, чтобы:

a) гарантировать, что система менеджмента информационной безопасности может достигать ожидаемых результатов;

b) предотвратить или уменьшить нежелательные эффекты;

c) обеспечить постоянное улучшение.

Студент должен планировать:

d) действия по обработке этих рисков и реализации возможностей; и

e) каким образом

1) встраивать эти действия в процессы системы менеджмента информационной безопасности и выполнять их; и

2) оценивать результативность этих действий.

#### Оценка рисков информационной безопасности

Студент должен определить и применять процесс оценки рисков информационной безопасности, который:

a) устанавливает и обеспечивает применение критериев оценки информационной безопасности, включающие в себя:

1) критерии приемлемости риска; и

2) критерии для оценки рисков информационной безопасности;

b) гарантирует, что производимые оценки рисков информационной безопасности дают непротиворечивые, обоснованные и сопоставимые результаты;

c) обеспечивает выявление рисков информационной безопасности:

1) применяет процесс оценки рисков информационной безопасности для идентификацию рисков, связанных с потерей конфиденциальности, целостности и доступности информации в рамках области применения системы менеджмента информационной безопасности; и

2) обеспечивает определение владельцев риска;

d) обеспечивает анализ рисков информационной безопасности:

1) оценку потенциальных последствий в том случае, если бы риски, идентифицированные при выполнении требований п. 6.1.2. (ISO/IEC 27001:2022) c) 1) реализовались ;

2) оценку реальной вероятности реализации рисков, идентифицированных при выполнении требований п. 6.1.2. (ISO/IEC 27001:2022) c) 1); и

3) определение уровня риска;

e) обеспечивает оценку рисков информационной безопасности:

1) сравнение результатов анализа рисков с критериями риска, установленными при выполнении требований п. 6.1.2. (ISO/IEC 27001:2022) а); и

2) расстановку рисков по приоритетам для последующей обработки рисков.

Студент должен оформить как документированную информацию данные, полученные в ходе процесса оценки рисков информационной безопасности.

Хххххх хххх хххххххх хххххх, ххххххх ххххххх х ххххх хххххх ххххх. Ххх хх хх ххххххх хххххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххх ххххххххх хххххххххх ххххххххх ххххххх. Хх хххххххх хххххххххх хххххххх ххххххх ххххххххххх ххх ххххххх ххххххх ххххх хххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххх ххххххххх хххххххххх ххххххххх ххххххх. Хх хххххххх хххххххххх хххххххх ххххххх ххххххххххх ххх ххххххх ххххххх ххххх хххххх ххххххх.

#### Обработка рисков информационной безопасности

Студент должен определить и выполнить процесс обработки рисков информационной безопасности, чтобы:

a) выбрать соответствующие методы обработки рисков информационной безопасности с учетом результатов оценки рисков;

b) определить любые средства управления, которые необходимы для реализации выбранных методов обработки рисков информационной безопасности;

c) сравнить средства управления, определенные при выполнении требований п. 6.1.3 b), с приведенными в приложении A (ISO/IEC 27001:2022), и удостовериться, что никакие из необходимых средств управления не были упущены из виду;

ПРИМЕЧАНИЕ. Приложение A содержит перечень возможных средств управления.

Пользователям данного документа дана ссылка на Приложение A с тем, чтобы гарантировать, что никакие необходимые средства управления не были пропущены.

ПРИМЕЧАНИЕ. Средства управления информационной безопасностью, перечисленные в Приложении A, не являются исчерпывающими и, если необходимо, могут быть добавлены дополнительные средства управления.

d) сформировать Заявление о применимости, которое содержит:

─ необходимые средства управления (см.6.1.3 b) и c)) (ISO/IEC 27001:2022);

─ обоснование их применения;

─ указание на то, применяются ли эти средства управления в данный момент или нет; а также

─ обоснование исключения любых средств управления, приведенных в Приложении A;

e) разработать план обработки рисков информационной безопасности; и

f) получить одобрение плана от владельцев риска и подтверждение принятия остаточных рисков информационной безопасности.

Студент должен оформить данные процесса обработки рисков информационной безопасности как документированную информацию.

ПРИМЕЧАНИЕ. Процессы оценки и обработки рисков информационной безопасности в данном документе согласованы с принципами и общими руководящими указаниями, приведенными в ISO 31000 [5].

Приложение A стандарта ISO/IEC 27001:2022:

Средства управления информационной безопасностью

|  |  |  |
| --- | --- | --- |
| **Организационные средства управления** | | |
|  | Политики информационной безопасности | Средство управления  Должны быть определены политика информационной  безопасности и политики по другим направлениям,  утверждены руководством, опубликованы, доведены до сведения и поняты соответствующим персоналом и  значимыми заинтересованными сторонами, а также  пересматриваться через запланированные интервалы  времени и в случае значительных изменений. |
|  | Роли и обязанности,  связанные с  информационной  безопасностью | Средство управления  Должны быть определены и назначены все роли и  обязанности, связанные с информационной безопасностью, в соответствии с потребностями  организации. |
|  | Разделение  обязанностей | Средство управления  Вступающие в противоречие друг с другом обязанности и области ответственности должны быть разделены. |
|  | Обязанности  руководства | Средство управления  Руководство должно требовать от всех сотрудников  соблюдения требований по информационной  безопасности в соответствии с установленными  политикой информационной безопасности, иными  политиками и процедурами организации. |
|  | Контакты с  полномочными  органами | Средство управления  Должны быть установлены и поддерживаться  соответствующие контакты с соответствующими  органами. |
|  | Контакты с  профессиональными  сообществами | Средство управления  Студент должен установить и поддерживать  контакты с профессиональными сообществами или  иными форумами специалистов по информационной  безопасности и профессиональными ассоциациями. |
|  | Изучение угроз | Средство управления  Должна собираться и анализироваться информация,  связанная с угрозами информационной безопасности, для изучения угроз |
|  | Информационная  безопасность в  управлении проектами | Средство управления  Обеспечение информационной безопасности должно быть интегрировано в управление проектами. |
|  | Инвентаризация  информации и иных  связанных с ней  активов | Средство управления  Реестры информационных и иных связанных с этим  активов, включая владельцев, должны быть разработаны и поддерживаться в актуальном состоянии |
|  | Надлежащее  применение  информационных и  иных, связанных с  ними, активов | Средство управления  Должны быть определены, документированы и внедрены правила надлежащего применения и процедуры обращения с информационными и иными, связанными с ними, активами |
|  | Возврат активов | Средство управления  Персонал и представители заинтересованных сторон,  насколько это применимо, должны вернуть все активы  организации в ее распоряжение при изменении или  прекращении трудовых отношений, контрактов и  соглашений. |
|  | Классификация  информации | Средство управления  Информация должна быть классифицирована исходя из  потребностей информационной безопасности организации на основе требований к конфиденциальности, целостности и доступности и требований заинтересованных сторон. |
|  | Маркировка  информации | Средство управления  Должен быть разработан и внедрен соответствующий набор процедур для маркировки информации в соответствии со схемой классификации информации, принятой в организации. |
|  | Передача информации | Средство управления  Должны быть внедрены правила, процедуры или соглашения для любого вида средств передачи как внутри организации, так и между организацией и другими сторонами |
|  | Управление доступом | Средство управления  Должны быть на основе требований бизнеса и требований к информационной безопасности разработаны и внедрены правила физического и логического доступа к информационным и иным, связанным с ними, активам |
|  | Управление  идентификацией | Средство управления  Должно быть обеспечено управление всем жизненным циклом идентификаторов |
|  | Информация для  аутентификации | Средство управления  Назначение и управление информацией для  аутентификации должно быть контролируемым в рамках процесса управления, включая консультирование сотрудников по вопросам надлежащего обращения с информацией для аутентификации |
|  | Права доступа | Средство управления  Права доступа к информационным и иным, связанным с  ними, активам должны быть предоставлены,  пересматриваться, изменяться и аннулироваться в  соответствии с различными политиками организации и  правилами контроля доступа |
|  | Информационная  безопасность в  отношениях с  поставщиками | Средство управления  Должны быть определены и внедрены процессы и  процедуры управления рисками для информационной  безопасности, связанными с использованием продуктов и услуг, предоставляемых поставщиками |
|  | Обеспечение  информационной  безопасности в рамках  соглашений с  поставщиками | Средство управления  Должны быть установлены сущностные требования к  информационной безопасности и согласованы с каждым поставщиком с учетом особенностей отношений с этим поставщиком. |
|  | Управление  информационной  безопасностью в  цепочках поставки в  сфере информационно-  коммуникационных  технологий (ИКТ) | Средство управления  Должны быть разработаны и внедрены процесс и  процедуры управления рисками для информационной  безопасности, связанных с цепочкой поставок продуктов и услуг ИКТ. |
|  | Мониторинг, анализ и управление  изменениями услуг  поставщиков | Средство управления  Студент должен регулярно вести мониторинг,  анализ, оценку и управлять изменениями в деятельности поставщиков в сфере информационной безопасности и поставки услуг. |
|  | Информационная  безопасность при  использовании  облачных сервисов | Средство управления  Должен быть установлен процесс запроса, использования, управления и прекращения использования облачных сервисов в соответствии с требования организации в области информационной безопасности. |
|  | Планирование и  подготовка в части  управления  инцидентами  информационной  безопасности | Средство управления  Студент должен планировать и готовиться к  управлению инцидентами информационной безопасности посредством определения, установления и информирования о процессах управления инцидентами информационной безопасности, ролях и обязанностях. |
|  | Оценка событий в  области  информационной  безопасности и  принятие решений | Средство управления  Студент должен оценивать события в области  информационной безопасности и решать, следует ли их  расценивать как инцидент информационной  безопасности. |
|  | Ответные меры по  инцидентам  информационной  безопасности | Средство управления  Реагирование на инциденты информационной  безопасности должно осуществляться в соответствии с  документированными процедурами. |
|  | Излечение уроков из  инцидентов  информационной  безопасности | Средство управления  Знания, полученные из инцидентов информационной  безопасности, должны использоваться для усиления и  улучшения средств управления информационной  безопасностью. |
|  | Сбор свидетельств | Средство управления  Студент должен установить и внедрить процедуры  для идентификации, сбора, накопления и сохранения  свидетельств, связанных с событиями информационной  безопасности. |
|  | Информационная  безопасность при сбое | Средство управления  Студент должен планировать, каким образом она  будет обеспечивать информационную безопасность на  соответствующем уровне при сбое. |
|  | Готовность ИКТ к  обеспечению  непрерывности  бизнеса | Средство управления  Меры по обеспечению готовности ИКТ должны  планироваться, внедряться, поддерживаться в  актуальном состоянии и тестироваться с точки зрения  целей непрерывности бизнеса и требований к  непрерывности функционирования ИКТ. |
|  | Законодательные,  нормативные и  контрактные  требования | Средство управления  Законодательные, нормативные и контрактные  требования, значимые для информационной  безопасности, а также подход организации к  удовлетворению этих требований должны быть  определены, документированы и сохраняться  актуальными. |
|  | Права  интеллектуальной  собственности | Средство управления  Студент должен осуществлять соответствующие  процедуры для защиты прав интеллектуальной  собственности. |
|  | Защита записей | Средство управления  Записи должны быть защищены от потери, повреждения, фальсификации, несанкционированного доступа и несанкционированной публикации. |
|  | Приватность и защита  персональных данных | Средство управления  Студент должен установить и выполнять  требования, связанные с сохранением приватности и  защитой персональных данных (ПД) в соответствии с  действующими законодательными, нормативными и  контрактными требованиями. |
|  | Независимый анализ  информационной  безопасности | Средство управления  Подход организации к управлению информационной  безопасностью и его реализация, в том числе. люди,  процессы и технологии, должны подвергаться  независимому анализу через запланированные  интервалы времени или в тех случаях, когда происходят  существенные изменения. |
|  | Соответствие  политикам, правилам и стандартам  информационной  безопасности | Средство управления  Соответствие политике информационной безопасности,  политикам в других областях, правилам и стандартам  должно регулярно анализироваться. |
|  | Документированные  операционные  процедуры | Средство управления  Операционные процедуры для устройств обработки  информации должны быть документированы и доступны персоналу, которому они требуются. |
| **Средства управления, связанные с персоналом** | | |
|  | Предварительная  проверка | Средство управления  Проверка при приеме на работу, осуществляемая для всех кандидатов, должна проводиться в рамках  соответствующих законодательных актов, регламентов и этических норм, а также должна быть соразмерна  бизнес-требованиям, категории информации по  классификации, к которой предполагается доступ, и  предполагаемым рискам. |
|  | Условия трудового  соглашения | Средство управления  Трудовые соглашения с сотрудниками должны  устанавливать их и организации ответственность в части информационной безопасности. |
|  | Осведомленность,  образование и  подготовка в сфере  информационной  безопасности | Средство управления  Сотрудники организации и значимые заинтересованные  стороны должны быть соответствующим образом  информированы, иметь соответствующее образование и  подготовку, а также регулярно извещаться об изменениях в политике информационной безопасности организации, политиках по другим направлениям, в той мере, насколько это важно для исполнения их служебных обязанностей. |
|  | Дисциплинарные меры | Средство управления  Должен быть разработан и доведен до сведения  персонала процесс для принятия мер к тем сотрудникам и иным заинтересованным сторонам, которые допустили нарушение требований информационной безопасности. |
|  | Обязанности после  прекращения или  изменения трудовых  отношений | Средство управления  Ответственность и обязанности по соблюдению  информационной безопасности, которые остаются в силе после прекращения или изменения трудовых отношений, должны быть определены и сообщены соответствующему персоналу и иным заинтересованным сторонам, а также обеспечено их выполнение. |
|  | Соглашения о  конфиденциальности  или неразглашении | Средство управления  Соглашения о конфиденциальности или неразглашении, отражающие потребности организации в защите информации, должны быть определены,  документированы, регулярно пересматриваться и быть  подписанными персоналом и иными заинтересованными сторонами. |
|  | Удаленная работа | Средство управления  Должны осуществляться меры по обеспечению  безопасности в тех случаях, когда персонал работает  удаленно, чтобы обеспечить защиту информации, к  которой есть доступ, которая обрабатывается или  хранится в местах за пределами организации. |
|  | Отчетность о событиях  информационной  безопасности | Средство управления  Студент должен иметь процедуру для персонала для своевременного информирования о выявленных или предполагаемых событиях информационный  безопасности посредством соответствующих каналов. |
| **Средства управления, связанные с физическим доступом** | | |
|  | Физические периметры  безопасности | Средство управления  Периметры безопасности должны быть определены и  использоваться для защиты зон нахождения информации и иных, связанной с ней, активов |
|  | Физический вход | Средство управления  Зоны безопасности должны быть защищены выделением мест прохода и соответствующими средствами контроля прохода . |
|  | Защита офисов,  помещений и  устройств | Средство управления  Меры физической защиты безопасности для офисов,  помещений и оборудования должны быть разработаны и применяться. |
|  | Мониторинг  физической защиты | Средство управления  Помещения должны находиться под постоянным  контролем неавторизованного доступа. |
|  | Защита от физических  и природных угроз | Средство управления  Должны быть разработаны и внедрены меры по защите  от физических и природных угроз, таких как стихийные  бедствия, а также иные намеренные или  непреднамеренные физические угрозы для  инфраструктуры. |
|  | Работа в защищенных  зонах | Средство управления  Должны быть разработаны и применяться процедуры для работы в защищенных зонах. |
|  | Чистый стол и чистый экран | Средство управления  Должны быть установлены и обеспечено выполнение  правил чистого стола для бумажных документов,  переносных устройств хранения информации и правил  чистого экрана для устройств обработки информации. |
|  | Размещение и защита  оборудования | Средство управления  Оборудование должно быть размещено в безопасном  месте и защищено. |
|  | Защита активов вне  территории | Средство управления  Активы, находящиеся вне территории организации,  должны быть защищены. |
|  | Устройства хранения | Средство управления  Управление устройствами хранения должно  осуществляться на всем протяжении их жизненного  цикла, включающего приобретение, использование,  транспортировку и уничтожение, в соответствии с  классификационной схемой организации и требованиями к обращению. |
|  | Службы обеспечения | Средство управления  Устройства обработки информации должны быть  защищены от перебоев в электроснабжении и других  сбоев, вызываемых перебоями в работе служб  обеспечения. |
|  | Защита кабельных  сетей | Средство управления  Питающие кабели и кабели, передающие данные или  обеспечивающие работу информационных сервисов,  должны быть защищены от перехвата, помех или  повреждения. |
|  | Обслуживание  оборудования | Средство управления  Оборудование должно обслуживаться надлежащим  образом, чтобы гарантировать конфиденциальность,  целостность и доступность информации. |
|  | Безопасная утилизация  или повторное  использование  оборудования | Средство управления  Элементы оборудования, содержащие накопители,  должны быть проверены, чтобы гарантировать, что  любые ценные данные и лицензионное программное  обеспечение удалены или надежным образом затерты  новой информацией до утилизации или повторного  использования. |
| **Технологические средства управления** | | |
|  | Оконечные устройства  пользователя | Средство управления  Информация сохраняемая, обрабатываемая или к которой имеется доступ через оконечные устройства  пользователя, должна быть защищена. |
|  | Привилегированные  права доступа | Средство управления  Предоставление и использование привилегированных  прав доступа должно быть ограничено и находиться под  контролем. |
|  | Ограничение доступа к  информации | Средство управления  Доступ к информации и иным, связанным с нею активам, должен быть ограничен в соответствии установленными политиками по контролю доступа. |
|  | Доступ к исходному коду | Средство управления  Должно быть обеспечено соответствующее управление  доступом на чтение и запись к исходному коду,  инструментам разработки и библиотекам. |
|  | Безопасная  аутентификация | Средство управления  Должны быть внедрены технологии и процедуры  безопасной аутентификации, основанные на  ограничениях доступа к информации и политиках по  контролю доступа. |
|  | Управление  производительностью | Средство управления  Использования ресурсов должно быть под контролем и  настроено в соответствии с текущими и перспективными требованиями к производительности. |
|  | Защита от вредоносного  программного  обеспечения | Средство управления  Должна быть внедрена защита от вредоносного  программного обеспечения и сопровождаться  соответствующим информированием пользователей. |
|  | Управление  техническими  уязвимостями | Средство управления  Должна получаться информация о технических  уязвимостях в используемых информационных системах, оцениваться возможное влияние на организацию таких уязвимостей и приниматься соответствующие меры. |
|  | Менеджмент  конфигураций | Средство управления  Конфигурации, включая те, что связаны с безопасностью, оборудования, программного обеспечения, сервисов и сетей должны быть определены, документированы, внедрены, вестись их мониторинг и анализ. |
|  | Удаление информации | Средство управления  Информация, хранящаяся в информационных системах, на устройствах или любых иных носителей данных, должна быть удалена, если она больше не требуется. |
|  | Маскирование данных | Средство управления  Должно использоваться маскирование данных в  соответствии с политиками организации по контролю  доступа и иными специализированными политиками, а  также требованиями бизнеса, с учетом применимого  законодательства. |
|  | Предупреждение утечки данных | Средство управления  Должны применяться меры по предупреждению утечки  данных в системах, сетях и иных устройствах для  обработки, хранения и передачи конфиденциальной  информации. |
|  | Резервное копирование  информации | Средство управления  Должно выполняться и регулярно тестироваться  резервное копирование информации, программного  обеспечения и систем в соответствии с принятой  политикой резервного копирования. |
|  | Избыточность устройств  обработки информации | Средство управления  Устройства обработки информации должны применяться с избыточностью, достаточной для выполнения требований по доступности. |
|  | Ведение журналов  (логов) | Средство управления  Журналы (логи), фиксирующие действия, исключения,  сбои и иные значимые события должны вестись,  сохраняться, быть защищенными и анализироваться. |
|  | Мониторинг действий | Средство управления  Должен осуществляться мониторинг сетей, систем и  приложений с целью выявления отклонений от  нормального поведения и принятие соответствующих  мер для оценки возможных инцидентов информационной безопасности. |
|  | Синхронизация часов | Средство управления  Время у информационных систем, используемых  организацией, должно быть синхронизировано с  одобренными источниками точного времени. |
|  | Использование утилит с  привилегированными  правами | Средство управления  Применение утилит, которые могли бы обходить средства контроля системы и приложений, должно быть ограничено и строго контролироваться. |
|  | Установка приложений в  операционной системе | Средство управления  Должны быть внедрены процедуры и меры для  безопасного управления установкой программного  обеспечения в операционной системе. |
|  | Безопасность сетей | Средство управления  Сети и сетевые устройства должны быть защищены,  управляться и контролироваться с целью защиты  информации в системах и приложениях. |
|  | Безопасность сетевых  сервисов | Средство управления  Должны быть определены, внедрены и контролироваться механизмы обеспечения безопасности, уровни сервиса и требования к обслуживанию сетевых служб. |
|  | Разделение сетей | Средство управления  Группы информационных сервисов, пользователей и  информационных систем должны быть разделены в сетях организации. |
|  | Веб-фильтрация | Средство управления  Должны быть определены и внедрены правила  результативного использования криптографии, включая управление криптографическими ключами. |
|  | Жизненный цикл  разработки безопасного  программного  обеспечения | Средство управления  Должны быть установлены и применяться правила  разработки безопасного программного обеспечения и  систем. |
|  | Применение требований  по безопасности | Средство управления  Должны быть выявлены, установлены и утверждены  требования по информационной безопасности для  разработки или приобретения приложений. |
|  | Безопасная архитектура  систем и принципы  разработки | Средство управления  Принципы разработки безопасных систем должны быть установлены, документированы, поддерживаться в актуальном состоянии и применяться к любым действиям в рамках разработки информационных систем. |
|  | Безопасное кодирование | Средство управления  Принципы создания безопасного кода должны  применяться в ходе разработки программного  обеспечения. |
|  | Тестирование  обеспечения  безопасности при  разработке и приемке | Средство управления  Процессы тестирования обеспечения безопасности  должны быть определены и внедрены в рамках  жизненного цикла разработки. |
|  | Разработка, переданная  на аутсорсинг | Средство управления  Студент должен управлять, осуществлять  мониторинг и анализ деятельности, связанной с  разработкой систем, переданной на аутсорсинг. |
|  | Разделение среды  разработки,  тестирования и  эксплуатации | Средство управления  Среда разработки, тестирования и рабочая среда должны быть отделены друг от друга и обеспечена безопасность. |
|  | Управление изменениями | Средство управления  Должны быть предусмотрены процедуры управления  изменениями в средствах обработки информации и  информационных системах. |
|  | Данные для  тестирования | Средство управления  Данные для тестирования должны быть  соответствующим образом отобраны, обеспечена их  защищенность и управление. |
|  | Защита информационных  систем в ходе аудита | Средство управления  Аудиты и иные действия, направленные на обеспечение гарантий, включающие оценку операционных систем, должны быть спланированы и согласованы проводящим тестирование и соответствующим руководством. |

Хххххх хххх хххххххх хххххх, ххххххх ххххххх х ххххх хххххх ххххх. Ххх хх хх ххххххх хххххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххх ххххххххх хххххххххх ххххххххх ххххххх. Хх хххххххх хххххххххх хххххххх ххххххх ххххххххххх ххх ххххххх ххххххх ххххх хххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххх ххххххххх хххххххххх ххххххххх ххххххх. Хх хххххххх хххххххххх хххххххх ххххххх ххххххххххх ххх ххххххх ххххххх ххххх хххххх ххххххх.

### Постановка задач (целей) в области информационной безопасности и планирование их достижения

Студент должен установить цели (задачи) в области информационной безопасности для соответствующих функций и уровней.

Цели (задачи) в области информационной безопасности должны:

a) быть согласованными с политикой информационной безопасности;

b) быть измеримыми (если возможно);

c) учитывать действующие требования к информационной безопасности, а также результаты оценки и обработки рисков;

d) отслеживаться с точки зрения их выполнения;

e) быть сообщены персоналу;

f) соответствующим образом обновляться;

g) быть доступны в документированной форме.

Студент должен оформить документированную информацию по целям (задачам) в области информационной безопасности как.

При планировании, каким образом достигнуть своих целей (задач) в области информационной безопасности, Студент должен определить:

a) что будет сделано;

b) какие ресурсы потребуются;

c) кто будет ответственным за выполнение;

d) когда цели будут достигнуты; и

e) как результаты будут оцениваться.

Хххххх хххх хххххххх хххххх, ххххххх ххххххх х ххххх хххххх ххххх. Ххх хх хх ххххххх хххххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххх ххххххххх хххххххххх ххххххххх ххххххх. Хх хххххххх хххххххххх хххххххх ххххххх ххххххххххх ххх ххххххх ххххххх ххххх хххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххх ххххххххх хххххххххх ххххххххх ххххххх. Хх хххххххх хххххххххх хххххххх ххххххх ххххххххххх ххх ххххххх ххххххх ххххх хххххх ххххххх.

Хххххх хххх хххххххх хххххх, ххххххх ххххххх х ххххх хххххх ххххх. Ххх хх хх ххххххх хххххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххх ххххххххх хххххххххх ххххххххх ххххххх. Хх хххххххх хххххххххх хххххххх ххххххх ххххххххххх ххх ххххххх ххххххх ххххх хххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххх ххххххххх хххххххххх ххххххххх ххххххх. Хх хххххххх хххххххххх хххххххх ххххххх ххххххххххх ххх ххххххх ххххххх ххххх хххххх ххххххх.

### Корректирующие действия в случае выявления несоответствий СМИБ требованиям

При выявлении несоответствия Студент должен:

a) реагировать на несоответствие и, насколько применимо:

1) принять меры для управления им и его исправления;

2) принять меры в отношении последствий;

b) оценивать потребность в действиях по устранению причины несоответствия с тем, чтобы оно не повторялось или не происходило в другом месте, посредством:

1) анализа несоответствия;

2) определения причин несоответствия, и

3) выявления, есть ли подобные несоответствия, или могли бы они потенциально произойти;

c) осуществлять любое необходимое действие;

d) анализировать результативность всех предпринятых корректирующих действий; и

e) вносить изменения в систему менеджмента информационной безопасности, если необходимо.

Корректирующие действия должны соответствовать последствиям выявленных несоответствий.

Студент должен оформить документированную информацию как свидетельство:

f) характера несоответствий и любых последующих предпринятых действий;

g) результатов любого корректирующего действия.

## Разработка программной части для СМИБ

### План разработки ПО

План должен содержать этапы разработки ПО, даты и ответственных лиц. План можно оформить в виде таблицы или диаграммы Ганта

Хххххх хххх хххххххх хххххх, ххххххх ххххххх х ххххх хххххх ххххх. Ххх хх хх ххххххх хххххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххх ххххххххх хххххххххх ххххххххх ххххххх. Хх хххххххх хххххххххх хххххххх ххххххх ххххххххххх ххх ххххххх ххххххх ххххх хххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххх ххххххххх хххххххххх ххххххххх ххххххх. Хх хххххххх хххххххххх хххххххх ххххххх ххххххххххх ххх ххххххх ххххххх ххххх хххххх ххххххх.

### Frontend-разработка

Продумайте дизайн своего приложения. Если вы внедряете существующее ПО, то проведите анализ его интерфейса

Если вы разрабатываете dll библитеку и у нее нет интерфейса – так и пишите, что ваша система не предполагает графический интерфейс

Однако, если у вас будет консольный интерфейс (текстовый) – его нужно показать в этом разделе

ВАЖНО – здесь не надо макетов и прототипов из преддипломной практики! Кратко описать процесс разработки интерфейса.

Хххххх хххх хххххххх хххххх, ххххххх ххххххх х ххххх хххххх ххххх. Ххх хх хх ххххххх хххххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххх ххххххххх хххххххххх ххххххххх ххххххх. Хх хххххххх хххххххххх хххххххх ххххххх ххххххххххх ххх ххххххх ххххххх ххххх хххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххх ххххххххх хххххххххх ххххххххх ххххххх. Хх хххххххх хххххххххх хххххххх ххххххх ххххххххххх ххх ххххххх ххххххх ххххх хххххх ххххххх.

Хххххх хххх хххххххх хххххх, ххххххх ххххххх х ххххх хххххх ххххх. Ххх хх хх ххххххх хххххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххх ххххххххх хххххххххх ххххххххх ххххххх. Хх хххххххх хххххххххх хххххххх ххххххх ххххххххххх ххх ххххххх ххххххх ххххх хххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххх ххххххххх хххххххххх ххххххххх ххххххх. Хх хххххххх хххххххххх хххххххх ххххххх ххххххххххх ххх ххххххх ххххххх ххххх хххххх ххххххх.

### Backend-разработка

Здесь вы должны показать как привязан ваш интерфейс к коду. И в целом, разработанный код

Если вы разрабатываете dll библитеку и у нее нет интерфейса – показываете только код.

Хххххх хххх хххххххх хххххх, ххххххх ххххххх х ххххх хххххх ххххх. Ххх хх хх ххххххх хххххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххх ххххххххх хххххххххх ххххххххх ххххххх. Хх хххххххх хххххххххх хххххххх ххххххх ххххххххххх ххх ххххххх ххххххх ххххх хххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххх ххххххххх хххххххххх ххххххххх ххххххх. Хх хххххххх хххххххххх хххххххх ххххххх ххххххххххх ххх ххххххх ххххххх ххххх хххххх ххххххх.

Хххххх хххх хххххххх хххххх, ххххххх ххххххх х ххххх хххххх ххххх. Ххх хх хх ххххххх хххххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххх ххххххххх хххххххххх ххххххххх ххххххх. Хх хххххххх хххххххххх хххххххх ххххххх ххххххххххх ххх ххххххх ххххххх ххххх хххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххх ххххххххх хххххххххх ххххххххх ххххххх. Хх хххххххх хххххххххх хххххххх ххххххх ххххххххххх ххх ххххххх ххххххх ххххх хххххх ххххххх.

Хххххх хххх хххххххх хххххх, ххххххх ххххххх х ххххх хххххх ххххх. Ххх хх хх ххххххх хххххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххх ххххххххх хххххххххх ххххххххх ххххххх. Хх хххххххх хххххххххх хххххххх ххххххх ххххххххххх ххх ххххххх ххххххх ххххх хххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххх ххххххххх хххххххххх ххххххххх ххххххх. Хх хххххххх хххххххххх хххххххх ххххххх ххххххххххх ххх ххххххх ххххххх ххххх хххххх ххххххх.

### Разработка модели доступа к данным

Здесь описать принцип разграничения прав доступа. Описать процесс разработки личных кабинетов пользователя и их функционал

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххх

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххх

### Тестирование разработанного ПО

Полное описание процесса тестирования у вас было в преддипломной практике. Здесь необходимо КРАТКО описать:

- какие методы тестирования использовались

- какие ошибки были найдены

- какие действия для исправления ошибок были предприняты

## План внедрения СМИБ (при необходимости добавить план развертывания ПО)

Планы внедрения и развертывания должны быть с датами и ответсвенными лицами. План можно оформить в виде таблицы или диаграммы Ганта

В плане внедрения СМИБ отразить пункты из блока «Обеспечение» ISO/IEC 27001:2022:

* **Компетентность**

Студент должен:

a) определять необходимую компетентность персонала, который выполняет работу под контролем организации, и который влияет на ее информационную безопасность;

b) гарантировать, что этот персонал компетентен в силу соответствующего образования, подготовки или опыта;

c) там, где это возможно, предпринимать меры для обеспечения необходимой компетентности и оценивать результативность предпринятых мер; и

d) сохранять соответствующую документированную информацию как доказательства компетентности.

ПРИМЕЧАНИЕ Возможные действия могут включать, например: обучение, наставничество или перемещение работающих сотрудников; или прием новых либо привлечение по контракту компетентных специалистов.

* **Осведомленность**

Персонал, выполняющий работу под контролем организации, должен быть осведомлен о:

a) политике в области информационной безопасности,

b) своем вкладе в результативность системы менеджмента информационной безопасности, включая выгоды от улучшения деятельности по обеспечению информационной безопасности, и

c) последствия невыполнения требований системы менеджмента информационной безопасности.

* **Коммуникация**

Студент должен определить потребность во внутренних и внешних коммуникациях, существенных для функционирования системы менеджмента информационной безопасности, включая:

a) на какой предмет обмениваться информацией,

b) когда обмениваться информацией;

c) с кем обмениваться информацией;

d) каким образом должна осуществляться коммуникация.

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххххххх ххххх ххххх хххххх ххххх хххххх ххххххх хххххх ххх ххх х хххх хх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Ххххх

## Руководство администратора программной части СМИБ

Для дальнейшей эксплуатации информационной системы, необходимо составить сопроводительный документ – “руководство администратора”.

Сама структура и все необходимые требования к содержанию руководства пользователя по ГОСТ 34, описаны в РД 50-34.698-90.

**Руководства выносятся в приложения!**

Руководство администратора представлено в Приложении 3.

Руководство пользователя представлено в Приложении 4.

## Документирование Политики информационной безопасности

Политика ИБ – это сборник правил и процедур защиты информации в организации. Документ может называться как «Политика информационной безопасности», так и «Правила и процедуры информационной безопасности» и т.п.

Структура документа представлена в Приложении 4.

**Политика выносится в приложения!**

Политика информационной безопасности представлена в Приложении 4.

## Выводы по главе 2

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх.

# ЭКОНОМИЧЕСКАЯ ЧАСТЬ

# ОБОСНОВАНИЕ ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ ОТ РАЗРАБОТКИ ИС

## Расчет затрат на разработку ИС

Далее идет ПРИМЕР:

ВАЖНО!!!!!!!! **ОБРАТИТЕ ВНИМАНИЕ, ЧТО ЭТО ВСЕГО ЛИШЬ МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ И ПРИМЕР ТИПОВОГО РАСЧЕТА!!!! Ctrl-C + Ctrl-V – НЕДОПУСТИМ!!!!**

## Выбор и обоснование методики расчёта экономической эффективности

При внедрении любой автоматизированной информационной системы (далее АИС), типовой или специально разработанной, в деятельность предприятия, важно понимать какие преимущества и выгоды оно получает. Если внедрение АИС не приносит пользы, оно нецелесообразно.

Для выпускной квалификационной работы, целью которой является разработка и/или внедрение АИС (модуля АИС), его эффективность будет равна эффективности от внедрения самой АИС или ее модуля, разработанной в ходе проектирования.

Целью разработки АИС или модуля должно стать именно достижение некоторого уровня эффективности, улучшение деятельности автоматизируемого объекта, получения различных преимуществ.

## Оценка затрат на разработку и внедрение АИС

Затраты на информационную систему возникают на всех этапах ее жизненного цикла: разработка, внедрение и эксплуатация.

В качестве одной из современных методик оценки затрат на информационную систему используется Total Cost of Ownership –совокупная стоимость владения.

TCO - методика, с помощью которой возможна оценка структуры затрат, связанных с использованием всех составляющих элементов информационной системы в период её жизненного цикла.

Фактически длительность жизненного цикла АИС, для предприятия на котором она внедряется, исчисляется с момента принятия решения об автоматизации до момента вывода АИС из эксплуатации. Она включает в себя этапы разработки, внедрения и эксплуатации (полезного использования). В общем случае срок полезного использования АИС определяется скоростью ее морального износа, на которую влияют:

* характеристики самой АИС (степень ее современности, использование передовых технологий);
* динамика и направление развития предприятия (смена рода деятельности предприятия может сделать АИС непригодной для дальнейшего использования);
* конъюнктура рынка ИТ (возникновение новых технологий и систем).

В рамках дипломного проекта можно оценить срок полезного использования АИС, исходя из анализа объекта дипломирования. Он может составлять от 1 до 5 лет. Длительность этапов разработки и внедрения оцениваются по фактическим данным или плану-графику работ.

Все затраты включаемые в TCO разделяются на капитальные и эксплуатационные. Капитальные осуществляются однократно на стадиях разработки и внедрения; текущие затраты являются необходимыми для поддержания работоспособности АИС с момента ввода в эксплуатацию и до ее завершения.

На практике предприятие, автоматизирующее свою деятельность, может использовать *программное обеспечение* *собственной разработки* или *решение* *сторонней фирмы-разработчика*.

В зависимости от варианта автоматизации (разработка собственной АИС или внедрение готового решения) состав затрат будет различным (см. таблица 2.30).

Таблица 2.30 – Состав затрат по методике TCO

|  | Собственная разработка | Внедрение готового решения |
| --- | --- | --- |
| **Этап разработки** | *Описание этапа*  Предпроектное обследование предприятия; подготовка технического задания; техническое и рабочее проектирование АИС; тестирование АИС.  *В состав затрат включают:*  - стоимость оборудования для разработки и затраты на его эксплуатацию в период разработки;  - стоимость ПО для проектирования и кодирования АИС; СУБД и прочее необходимое разработчику ПО;  - оплату труда проектировщиков и разработчиков;  - затраты на содержание и обслуживание помещений \*;  - прочие расходы;  - косвенные расходы. | *Описание этапа*  Предпроектное обследование предприятия; подготовка технического задания; анализ рынка АИС; выбор и приобретение АИС.  *В состав затрат включают:*  - стоимость программного обеспечения (выбранная АИС и дополнительное ПО, например СУБД);  - заработную плату сотрудников, выполнявших обследование, анализ рынка и т.п.;  - оплату услуг в сфере консалтинга;  - затраты на командировочные расходы и т. д. |
| **Этап внедрения** | *Описание этапа:*  Установка прикладного ПО; настройка ПО; обучение персонала.  *В состав затрат включают:*  - стоимость оборудования (рабочие места пользователей);  - оплату труда по установке;  - затраты на обучение персонала;  - затраты на содержание и обслуживание помещений. | *Описание этапа:*  Установка прикладного ПО; доработка и настройка ПО; обучение персонала.  *В состав затрат включают:*  - стоимость оборудования (рабочие места пользователей);  - стоимость доработки ПО;  - оплату труда сотрудников;  - затраты на обучение персонала;  - затраты на содержание и обслуживание помещений. |
| **Этап эксплуатации** | *В состав затрат включают:*  - оплату труда персонала, обеспечивающего эксплуатацию (сисадмин, сотрудники ИТ-служб);  - затраты на профилактические работы;  - затраты на содержание и обслуживание помещений;  - затраты на профилактические работы;  - стоимость сбоев и простоев АИС. | *В состав затрат включают:*  - оплату труда персонала, обеспечивающего эксплуатацию (сисадмин, сотрудники ИТ-служб);  - стоимость обновления лицензионного ПО;  - стоимость услуг по сопровождению ПО сторонними фирмами;  - затраты на профилактические работы;  - стоимость сбоев и простоев АИС;  - затраты на содержание и обслуживание помещений. |
| \* затраты на содержание и обслуживание помещений включают расходы на ремонт, коммунальные платежи, налоговые платежи, охрану, уборку и т.д. | | |

Поясним подробнее расчет совокупной стоимости владения, когда АИС разрабатывается собственными силами.

### Затраты на этапе разработки информационной системы

Затраты предприятия на этапе разработки являются единовременными и не зависят от длительности жизненного цикла.

В рамках дипломного проектирования, когда предметом дипломирования является разработка АИС для решения проблем конкретного предприятия, затраты на создание программного продукта оцениваются именно таким образом. Студент рассматривается как привлеченный ИТ-специалист.

В расходы этапа разработки обычно включают затраты на оборудование и специализированное программное обеспечение, оплату труда, начисления на заработную плату и другие расходы, в соответствии с методикой калькулирования себестоимости.

Затраты на **оборудование** (компьютерная техника, печатные устройства, специализированное оборудование) и **специализированное** ПО (средства проектирования, среда разработки, СУБД и т.д.) включаются в стоимость АИС полностью или частично. При отнесении прямых капитальных вложений на стоимость АИС необходимо учитывать направления их использования. Например, для разработки АИС необходимо приобрести лицензионное программное обеспечение (среду разработки). Если приобретенное программное обеспечение используется для разработки только этой АИС, то стоимость среды разработки полностью должна быть отнесена к прямым капитальным вложениям. Если приобретенное лицензионное ПО будет использовано разработчиком для реализации и других проектов, то к оцениваемой разработке можно отнести часть затрат по приобретению означенного ПО. Долю затрат относимую на текущую разработку можно определить исходя из трудоемкости проектов, размера ФОТ основного персонала или других соображений.

Для разработок «собственными силами», в том числе, когда речь идет о дипломном проекте, специализированное ПО приобретается преимущественно только для одного проекта, т.к. разработка АИС не является основным направлением деятельности предприятия.

Затраты на **оплату труда** определяются как повременная оплата исходя из количества затраченных рабочих человеко-часов на каждом этапе разработки и среднечасовой ставки исполнителей, с учетом их квалификации:

Где n – количество выделенных этапов работ, чем более детально представлен процесс разработки, тем точнее можно оценить трудозатраты;

T*i* – количество человеко-часов на выполнение i-го этапа;

R*j* – почасовая расценка на j-й вид работ.

**Начисления на фонд оплаты труда** определяется как произведение определенного ранее фонда оплаты труда и ставки отчислений во внебюджетные фонды.

**Затраты на содержание и обслуживание помещений** учитываются отдельной статьей, если для разработки привлечены дополнительные площади. Все затраты связанные с привлечением площадей (аренда, оплата коммунальных услуг, охраны и т.д.) включаются в стоимость разработки. Если используются уже имеющиеся площади предприятия, то затраты на них обычно входят в состав косвенных расходов (см. ниже).

**Прочие расходы** определяются по фактически затраченным суммам (или их сметной оценке) на приобретение канцелярских товаров, расходных материалов, консалтинговые услуги, командировочные расходы и другим прямым затратам, связанным с разработкой АИС.

**Косвенные расходы** – расходы, связанные с управлением и обеспечением выполнения основного процесса. Их появление обусловлено выполнением разных основных процессов в течение одного периода (например, разрабатываются разные АИС под общим управлением; предприятие кроме разработки АИС реализует и другие виды деятельности). Эти расходы учитываются в стоимости АИС пропорционально показателю, установленному отрасле­вой инструкцией по планированию себестоимости. Они распределяются между видами продукции (процессами) пропорционально условно выбранной базе распределения. Для разработки АИС наиболее целесообразно использовать в качестве базы распределения прямые расходы на оплату труда.

### Затраты на этапе внедрения

Начинается после завершения разработки АИС - подписания акта сдачи/приемки. На этом этапе выполняется весь комплекс работ, позволяющий организовать промышленную эксплуатацию АИС, в т.ч. установка и настройка прикладного программного обеспечения, организация рабочих мест, обучение персонала.

В состав затрат на внедрение должны быть включены:

* оплата сторонних специалистов, участвующих в установке, первоначальной настройке АИС. Поскольку при внедрении дипломной разработки, студент выступает как привлеченный специалист, оплата его труда за внедрение учитывается в этой статье;
* повременная оплата труда собственных специалистов, которые участвуют во внедрении и приемке системы;
* затраты на дополнительное оборудование и специализированное программное обеспечение, которое потребуется заказчику для организации работы внедряемой АИС (средства проектирования и разработки АИС учитываются в затратах на разработку). Если разработка велась собственными силами и некоторое специализированное ПО (например СУБД), необходимое для работы АИС уже было приобретено и учтено на этапе разработки, то повторно его стоимость не учитывается. Затраты этой категории носят капитальный характер и учитываются в TCO полностью;
* затраты на обучение сотрудников предприятия работе с новой АИС. Они должны включить стоимость платных курсов, учебных материалов, которые оплачиваются предприятием отдельно. Также необходимо включить стоимость рабочего времени, которое сотрудники затрачивают на обучение, если оно организовано в рабочее время, поскольку свои прямые обязанности сотрудники в это время не исполняют;
* прочие затраты;
* косвенные расходы.

Затраты на внедрение АИС выполняются один раз и не зависят от длительности жизненного цикла.

### Затраты на этапе эксплуатации

Затраты на этом этапе выполняются в течение всего жизненного цикла или оцениваемого временного периода. Они определяются в расчете на год, квартал или месяц (обычно год). В них включаются:

* затраты на оплату труда сотрудников фирмы непосредственно занятых сопровождением АИС (администратор АИС, программисты);
* затраты на профилактические работы;
* затраты содержание помещений, дополнительно занятых в связи с внедрением АИС;
* стоимость аварий и простоев предприятия, связанных с отказами АИС. Один из способов определения этих затрат основан на расчете суммы страховых платежей. Отказ АИС во время эксплуатация по каким-либо причинам носит вероятностный характер и может служить объектом страхования. В этом случае страховая сумма может быть определена как сумма потенциального ущерба от непредвиденных ситуаций. Чтобы переложить эти риски на страховую компанию предприятие (объект автоматизации) может заключить страховой договор. Тогда стоимость рисков будет равна страховым платежам, осуществляемым страхователем.

## Эффект от внедрения АИС

В общем случае под эффектом от внедрения понимаются некоторые позитивные изменения в объектах и процессах, которые связанные с внедряемой АИС. Такие позитивные изменения называют источниками эффекта, они обязательно хотя бы частично должны быть обусловлены именно внедрением АИС.

Приведем несколько примеров.

**Пример 1**

На предприятии внедрена АИС по работе с дебиторами, которая позволяет подбирать условия контрактов для каждого клиента, исходя из его характеристик и истории взаимодействия с ним; вести «черный список» контрагентов; оповещать клиентов о сроках наступления платежей по электронной почте. Это приводит к сокращению срока и общего объема дебиторской задолженности, то есть абсолютному и относительному высвобождению оборотных средств. В конечном счете, возможно увеличение коэффициента оборачиваемости и рост прибыли, в том числе и за счет экономии на оплате процентов по кредиту. Ведь в случае повышения оборачиваемости, предприятию не придется прибегать к кредитованию.

**Пример 2**

В школе внедряется система on-line информирования родителей об успеваемости и посещаемости учеников через сайт школы. Имея полную информацию, родители смогут своевременно реагировать на снижение успеваемости или прогулы ребенка и предпринимать меры воспитательного воздействия. В результате возможен рост успеваемости, который будет выражаться в увеличении среднего балла по итоговым отметкам школьников.

Конечно, программное обеспечение, каким бы оно ни было совершенным, не способно самостоятельно привести к указанным в примерах улучшениям. Для этого действует целый комплекс факторов. Соответствующие процессы необходимо организовать. Для первого примера необходимо чтобы сотрудники полностью соблюдали выработанные правила взаимодействия с клиентами, аккуратно вели историю взаимоотношений с клиентами. Для второго примера требуется организовать работу преподавателей по заполнению «электронных журналов», кроме того нужна заинтересованность родителей в подобной информации и их готовность оперативно принимать меры воспитательного характера к отстающим ученикам. Но без применения нового программного обеспечения эти процессы организовать было бы невозможно или затраты на их организацию были бы очень велики.

Таким образом, эффект от внедрения информационной системы на предприятии (в организации) выражается в улучшении каких-либо значимых показателей его работы. К таким показателям относится, например, прибыль, валовый или товарный выпуск продукции, реализация, себестоимость продукции или другие затраты, производительность труда и т.д. Если показатели, по которым достигается улучшение значений в связи с внедрением АИС, экономические, то и эффект называют экономическим.

Как видно из примеров эффект от внедрения АИС может носить не только экономический характер. Если АИС разработана для некоммерческой организации, которая не нацелена на получение прибыли, то получение экономического эффекта и не является первостепенной задачей - наличие экономического эффекта при внедрении АИС необязательно.

В настоящее время, кроме экономического эффекта, выделяют социальный, научный, демографический и другие виды эффекта.

Характеризуя любой из перечисленных видов эффекта от внедрения АИС, следует в первую очередь перечислить его источники и подробно описать взаимосвязь возникающего эффекта именно с внедрением разработанной АИС. Каждый источник эффекта должен выражаться некоторым измеримым показателем. Для первого примера такими показателями могут быть длительность оборота оборотных средств или прибыль. Для второго примера можно использовать такие показатели как средний балл учащихся или количество пропусков. Такие показатели можно назвать целевыми, их значения оцениваются на основе фактических данных о работе организации.

На практике эффект от внедрения АИС необходимо оценить еще до начала процесса внедрения, поскольку эта информация служит основой для принятия решения о разработке или приобретении АИС вообще. Поэтому используются плановые, прогнозные, предпочтительные значения.

Если возможно, то для каждого источника эффекта нужно указать целевой показатель и его плановое значение.

Эффективность проекта нужно оценивать на всем протяжении жизненного цикла, как и затраты.

## Экономический эффект

Говоря об оценке внедренческих проектов, часто употребляют слово „выгода“. В общем случае под выгодой подразумеваются некоторые позитивные явления, помогающие компании упрочить свое положение. Можно выделить четыре главных фактора, способствующих достижению этой цели:

* повышение функциональных характеристик и качества выпускаемой продукции;
* улучшение обслуживания клиентов;
* снижение операционных расходов;
* улучшение использования активов.

Экономический эффект может быть рассмотрен как прямая экономия ресурсов, возникшая вследствие внедрения АИС (экономия рабочего времени, экономия материалов и т.д.) в стоимостном выражении за определенный период.

Другой источник экономического эффекта это рост доходов предприятия за определенный период времени. Такой эффект можно определить, например, когда АИС внедряется в каналах сбыта и увеличивает пропускную способность канала. Тогда количество обслуженных клиентов увеличивается и растут доходы предприятия:

Если на основании расчетов не может быть получена общая стоимостная оценка эффекта, то экономический эффект может быть выражен в улучшении ключевых показателей деятельности предприятия (сумма прибыли, рентабельность, фондоотдача, выручка, материалоотдача, производительность труда и т.д.).

Существует целый ряд подходов к оценке эффективности внедрения АИС. Один из них носит название Rapid Economic Justification (REJ) - быстрое экономическое обоснование. Его используют для определения потенциальных выгод предприятия от автоматизации.

Оценка возможных эффектов от использования информационных систем и технологий в рамках этой методики проходит в пять шагов:

1. Оценка бизнеса – выделяются стратегические цели компании, их можно декомпозировать до уровня понятных «повседневных» проблем и задач. По каждой стратегической цели следует выделить ключевые показатели эффективности. Показатели эффективности должны быть измеримыми, процедура получения их значений – понятна, они должны количественно выражать степень достижения цели. В созданном перечне задач можно указать автоматизированные полностью, частично и неавтоматизированные.
2. Понимание решений – вырабатываются способы решения означенных ранее проблем, в том числе и с использованием АИС и ИТ. В большей степени можно сконцентрироваться на не полностью автоматизированных задах. Нужно понимать, что внедрение АИС может быть недостаточно для полного решения проблемы, необходимо сочетание с другими мероприятиями.
3. Понимание баланса – выполняется оценка улучшений, которые будут получены за счет реализации выбранных решений задач. Расчет количественных показателей производится на основе прогноза качественного улучшения протекания процессов на предприятии. Оценка качественных улучшений выполняется экспертным путем. Для преобразования качественных показателей в количественные используются методы классического экономического анализа. Улучшения определяются в двух направлениях: рост доходов и снижение расходов. Также на этом шаге оцениваются затраты на АИС по методике TCO.
4. Понимание рисков – предполагается по каждому решению оценить риски в координатах «вероятность - степень влияния», которые могут не позволить получить спрогнозированные качественные улучшения, и предлагаются мероприятия по их снижению.
5. Понимание финансовых метрик – на этом этапе нужно определить показатели эффективности такие как чистый приведенный доход, рентабельность, срок окупаемости.

Результаты работы на каждом шаге принято обобщать в виде таблиц.

Применение методики REJ в рамках оценки эффективности дипломного проекта возможно в несколько совращенном варианте: на первом шаге можно выделять только те стратегии и показатели эффективности, на которые разрабатываемая АИС окажет влияние; возможно в список рисков на четвертом шаге включить только основные. Пример применения методики приведен в приложении А.

## Социальный эффект

Социальная результативность внедрения АИС определяется динамикой индикаторов, отражающих качество труда сотрудников предприятия и жизни населения, на которую оказывает влияние предприятие.

Одним из основных показателей по улучшению труда сотрудников фирмы, связанному с внедрением АИС, будет степень автоматизации:

Для примера автоматизации информирования родителей учеников средней школы об успеваемости через Internet, выделенный эффект – рост успеваемости учеников – будет носить социальный характер. Для каждой предметной области возможно выделить свои социальные показатели.

К социальному эффекту можно отнести и улучшение психологического климата в коллективе.

## Научный эффект

Научная результативность внедрения АИС измеряется динамикой индикаторов разработки и внедрения новых научных достижений:

- внедрение прогрессивных методов управления;

- внедрение новых методов обработки информации.

## Организационный эффект

Выражается в повышении управляемости предприятия, а именно в улучшении качества или увеличении количества управленческих решений. Описывая организационный эффект, необходимо перечислить управленческие решения, на принятие которых повлияет АИС. Нужно описать взаимосвязь между функциями АИС и управлением.

## Эффективность внедрения АИС (ПО ПРИМЕРУ)

Показатели эффективности выражают отношение достигнутого уровня эффекта к затратам на его достижение. Применительно к АИС затраты, это суммы расходов на разработку и внедрение оцененные по методике TCO. Эффект, это выраженное в стоимостных (рубли) или натуральных (часы, штуки и т.д.) единицах улучшение в работе предприятия, достигнутое за счет внедрения АИС:

Выделяют частные показатели, оценивающие эффективность проекта:

* чистый приведенный доход:

,

где NPV – чистый приведенный доход;

IC – начальные инвестиции (стоимость этапа разработки и внедрения);

CF*t* – годовой доход, определяемый как разница между дополнительной прибылью и дополнительными расходами (эксплуатационными затратами);

*i* – ставка дисконтирования.

* Внутренняя норма доходности (IRR) определяется на основе предыдущей формулы. При этом NPV полагается равной 0.
* Окупаемость инвестиций (ROI), показывает сколько раз на период (год) инвестиции в АИС вернуться в виде прибыли:

Срок окупаемости величина обратная ROI, показывает сколько лет понадобится для возврата инвестиций в виде дохода. Можно выразить срок окупаемости в месяцах.

По перечисленным показателям можно сделать вывод о целесообразности разработки или приобретения АИС. Внедрение может быть названо эффективным, если есть положительный чистый приведенный доход, срок окупаемости меньше, чем срок полезного использования

## Расчёт показателей экономической эффективности проекта (ПО ПРИМЕРУ)

Результаты расчета показателей экономической эффективности проекта необходимо представить в форме таблиц, графиков, повышающих наглядность восприятия. Здесь же следует определить улучшение качественных характеристик процесса управления соответствующим объектом и оценить влияние автоматизированного комплекса задач на эффективность деятельности органов управления и конечные результаты.

После расчета срока окупаемости проекта, все показатели эффективности должны быть проиллюстрированы диаграммами (например, круговыми или столбчатыми).

Приведем пример подобного расчета по методике REJ.

Рассмотрим предприятие, работающее в сфере оптовой торговли, имеющее большое количество средних и мелких клиентов. С большинством клиентов предприятие заключает долгосрочные договора, по которым в том числе предусматривается отпуск товаров с отсроченной оплатой, т.е. в кредит. Наличие таких условий в договорах является для фирмы одним из конкурентных преимуществ, от которого оно не может отказаться. Предприятию необходимы оборотные средства в большом объеме для поддержания широкого ассортимента предлагаемых товаров и необходимого уровня запасов. Для покрытия дефицита оборотных средств фирма часто обращается в банки за краткосрочными кредитами, средняя ставка по которым составляет 11,6%.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Тип клиентов | Кол-во клиентов / Кол-во договоров | Средний годовой оборот, тыс. руб. | Сумма дебиторской задолженности, всего по группе, тыс. руб. | Средний срок задолженности, дней |
| Крупные клиенты | 20 / 20 | 1 000 | 500 | 15 |
| Средние клиенты | 100 / 95 | 300 | 1 000 | 40 |
| Мелкие клиенты | 500 / 300 | 100 | 5 000 | 60 |

Рентабельность продаж фирмы за прошедший год составила 40%, средний уровень торговой наценки – 65%, объем привлеченных кредитных средств – 25 млн.руб. ПО данным бухгалтерского учета сумма долгосрочной дебиторской задолженности фирмы составляет 800 тыс.руб., списано безнадежных долгов 100 тыс.руб.

Стратегической целью компании является увеличение занимаемой доли рынка. Цель может быть декомпозирована на следующие подцели: увеличение среднего оборота по каждой группе клиентов и увеличение общего количества клиентов. Достижению и первой, и второй цели может способствовать расширение ассортимента предлагаемой продукции – это и привлечет новых клиентов и будет стимулировать уже имеющихся к большему объему закупок. Поддержание более широкого ассортимента товаров потребует больших вложений в оборотные средства, т.к. будет сопряжено с ростом складских запасов. Источником увеличения оборотных средств, которые будут вложены в создание дополнительного объема складских запасов, может стать сокращение дебиторской задолженности. Однако организация работы с клиентами на сегодняшний день не позволяет эффективно контролировать состояние дебиторской задолженности. В связи с этим фирма рассматривает возможность автоматизации данного процесса.

Рассмотрим порядок применения методики REJ для оценки эффективности автоматизации работы с дебиторской задолженностью.

**Шаг 1.** Исходя из изложенных выше соображений, можно составить таблицу, отражающую связь между целями фирмы и проблемами:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Фактор успеха | Ключевой показатель эф-ти | Стратегия | Проблема | Цель |
| Увеличение доли фирмы на рынке | Темп прироста объема продаж | Расширение ассортимента предлагаемых товаров | Недостаток средств для создания большего объема запасов | Сокращение неликвидных запасов |
| Сокращение текущих затрат |
| **Сокращение дебиторской задолженности** |

В качестве показателя эффективности выделен темп прироста объема продаж, а не доля фирмы на рынке, поскольку в конечном счете доля фирмы на рынке будет увеличиваться если темп роста реализации будет выше темпов роста рынка. Определение темпов прироста реализации для фирмы задача тривиальная. Этот показатель может быть рассчитан оперативно и служить реальным ориентиром для компании.

Далее сконцентрируемся на одной из представленных целей – сокращении дебиторской задолженности. Остальные цели можно проанализировать аналогичным образом.

|  |  |  |
| --- | --- | --- |
| Цель | Задачи 1 | Задачи 2 |
| Сокращение дебиторской задолженности | Контроль над сроками и условиями исполнения контрактов | Ведение реестра клиентов и условий контрактов |
| Уведомление дебиторов о сроках наступления платежей |
| Определение дебиторов, по которым возможно судебное решение вопроса |
| Контроль над условиями заключения новых контрактов | Разработка регламента работы с "проблемными" дебиторами |
| Ведение "черного списка" клиентов |

Кроме перечня задач второго уровня можно указать степень их автоматизации. Для рассматриваемого примера будем считать, что все задачи не автоматизированы, кроме ведения реестра клиентов (без указания условий контрактов).

**Шаг 2.** На втором шаге необходимо определиться, какие действия (решения) фирма могла бы предпринять для решения всех задач второго уровня. Один из вариантов представлен в таблице.

|  |  |  |
| --- | --- | --- |
| Задачи 2 | Решения | Результат |
| Уведомление дебиторов о сроках наступления платежей | Автоматическая рассылка электронных писем | Сокращение срока дебиторской задолженности на 40% |
| Формирование графика звонков |
| Ведение реестра клиентов и условий контрактов | Оперативная регистрация и получение информации об условиях контракта по любому клиенту |
| Определение дебиторов, по которым возможно судебное решение вопроса о взыскании задолженности | Формирование списка "злостных" неплательщиков | Сокращение суммы долгосрочной дебиторской задолженности на 30% |
| Подготовка документов для передачи в суд (акты сверки, перечень напоминаний и претензий и т.п.) |
| Разработка регламента работы с "проблемными" дебиторами | Определение порядка и условий работы с клиентами, допускавшими просрочки платежей | Снижение суммы списанных долгов на 80% |
| Ведение "черного списка" клиентов | Оперативное получение перечня клиентов-неплательщиков |
| Автоматический запрет на регистрацию контрактов с недобросовестными клиентами |

Результат от реализации предложенных решений на этапе подготовки к внедрению АИС может быть получен только экспертным путем в ходе консультаций с различными специалистами фирмы. Фактически, если способом реализации решений является внедрение АИС, то в колонке «Решения» предыдущей таблицы содержатся функции АИС.

**Шаг 3.** Задачей третьего шага является переход от прогнозируемых качественных улучшений работы фирмы к их количественной оценке. Для этого применяются методы классического экономического анализа, в том числе метод цепных подстановок.

В рассматриваемом примере для определения количественных выгод необходимо знать:

- сумму и сроки дебиторской задолженности в годовом исчислении;

- сумму долгосрочной дебиторской задолженности по итогам года;

- сумму безнадежных долгов, списанных по данным бухгалтерского учета.

Рассчитаем дополнительный приток денежных средств, учитывая данные предприятия и сокращение срока дебиторской задолженности на 40%. Если для всех групп клиентов сокращение срока дебиторской задолженности произойдет в равной степени, то фирма дополнительно получит в свое распоряжение всю сумму дебиторской задолженности на время равное 40% от срока задолженности. Фирма сэкономит на платежах процентов по кредиту, ведь эти сумму не придется занимать у банка.

Для крупных клиентов экономия составит тыс. руб.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Тип клиентов | Сумма деб. задолженности, тыс. руб. | Средний срок задолженности, дней | | Экономия на платежах %, тыс.руб. |
| до решения | после решения |
| Крупные клиенты | 500 | 15 | 9 | 0,953 |
| Средние клиенты | 1 000 | 40 | 24 | 5,085 |
| Мелкие клиенты | 5 000 | 60 | 36 | 38,137 |
| Итого: | | | | 44,175 |

Сокращение суммы долгосрочной дебиторской задолженности на 30% позволит предприятию высвободить для оборота 800\*0,3=240 тыс. руб.

Снижение суммы списанных долгов на 80% позволит предприятию высвободить для оборота 100\*0,8=80 тыс. руб.

Таким образом, годовой объем высвобождаемых средств составит 364,175 тыс. руб. Предполагая, что все высвободившиеся средства будут направлены на увеличение закупок товаров для продажи, то можно ожидать прироста выручки (объема продаж в стоимостном выражении) с учетом среднего уровня торговой наценки 364,175\*1,65=600,889 тыс.руб. Учитывая, что объем продаж фирмы составляет 100 млн. руб., темп прироста объема продаж за счет автоматизации будет 600,889/100000\*100%=0,6%

Дополнительная валовая прибыль, которую получит фирма с учетом рентабельности продаж составит 600,889\*0,4=240,356 тыс.руб.

После определения эффектов нужно оценить затраты на реализацию предлагаемых решений. Когда речь идет о внедрении АИС, выполняется оценка ее стоимости по методике TCO. Совокупная стоимость владения определяется на период 3 года.

|  | Статьи затрат | Расчет |
| --- | --- | --- |
| **Этап разработки** | Разработку модуля по работе с дебиторской задолженностью предприятие ведет силами собственного отдела ИТ. Время разработки АИС от формирования технического задания до завершения тестирования составляет 6 месяцев.  Для работы над проектом выделена группа из 2 программистов, которые выполняют весь перечень работ по проектированию, кодированию и отладке ПО. Их рабочие места оборудованы персональными компьютерами (ПК), инвентарная стоимость которых 50 тыс.руб. Разработка ведется в среде C# (приобретается подписка MS Visual Studio сроком на 1 год); проектирование - MS Visio Pro (имеется установленная версия, используемая в повседневной работе); системное ПО установлено на ПК и используется совместно с ними (входит в стоимость ПК); СУБД MS SQL Server 2012 (стоимость 440 тыс. руб.) установлена на сервере предприятия, функционирует круглосуточно и уже используется бухгалтерским приложением (6 рабочих мест), модулем складского учета (4 рабочих места) и модулем логистики (2 рабочих места). | |
| Стоимость оборудования для разработки и затраты на его эксплуатацию в период разработки | Учитывая, что ПК используются предприятием и вне разработки АИС, на стоимость разработки можно отнести только часть их стоимости, пропорционально времени использования, исходя из срока полезной эксплуатации (5 лет):  Затраты на эксплуатацию оборудования включаются в косвенные расходы. |
| Стоимость ПО для проектирования и кодирования АИС; СУБД и прочее необходимое разработчику ПО | - Стоимость подписки MS Visual Studio включается полностью в состав затрат, поскольку ее использование в других проектах не предусматривается. Она составляет **44 тыс. руб.**  - Стоимость MS Visio Pro учитывается в затратах пропорционально сроку использования (3 года), поскольку применяется для решения и других задач:  - Стоимость СУБД распределяется между различными приложения, использующими ее, пропорционально количеству рабочих мест (всего без учета этого проекта 12) и сроку эксплуатации (3 года). На период разработки рабочих мест - 2. |
| Оплата труда проектировщиков и разработчиков | - Программисты, занятые в проекте, оплачиваются повременно, исходя месячного оклада 25000 руб.  - Начисления на их заработную плату составят 30,6% от фонда оплаты: |
| Затраты на содержание и обслуживание помещений, в т.ч. охрану.  Прочие расходы. | Учитываются в составе косвенных затрат. |
| Косвенные расходы | Сумма косвенных расходов, относимая на ИТ службу предприятия, ежемесячно составляет 20 тыс. руб. ФОТ подразделения – 120 тыс. На стоимость проекта будет отнесено: |
| **Итого затраты на этапе разработки** | | **467 276 руб.** |
| **Этап внедрения** | Внедрение АИС будет осуществляться силами программистов, выполнявших разработку. Рабочее место пользователя дополнительно оснащается принтером. Обучение работе с АИС проводится в рабочее время. | |
| Стоимость оборудования (рабочие места пользователей) | Принтер – **5000 руб.** |
| Оплата труда по установке | Установка АИС займет 1 час. Стоимость часа работы программиста (количество часов в месяце в среднем 168): |
| Затраты на обучение персонала | Обучение займет 4 часа работы программиста и пользователя (при часовой ставке пользователя 110 руб.) |
| Затраты на содержание и обслуживание помещений, в т.ч. охрану. | Отсутствуют, поскольку не предусмотрено привлечение дополнительных площадей. |
| **Итого затраты на этапе внедрения** | | **6 190 руб.** |
| **Этап эксплуатации** | Эксплуатационные затраты определяем в годовом исчислении. | |
| Оплата труда персонала, обеспечивающего эксплуатацию (сисадмин, сотрудники ИТ-служб); | Время обслуживания АИС в среднем составляет 1 час в течение рабочего дня (247 рабочих дней в год), отсюда: |
| Затраты на профилактические работы | Профилактические работы выполняются 1 раз в месяц в течение 1 часа:  Расходные материалы (по смете) – 10 \*12=**120** руб. |
| Затраты на содержание и обслуживание помещений, в т.ч. охрану | Отсутствуют. |
| Стоимость сбоев и простоев АИС | Экономические потери предприятие понесет в случае простоя АИС в течение 5 и более рабочих дней (возможность заключения сделок с контрагентами из «черного списка», несвоевременное оповещение дебиторов о сроках наступления платежей). Сумма ущерба оценивается экспертно исходя из соображений, учтенных при расчете эффекта АИС, и составит 50 тыс.руб. в годовом исчислении. Вероятность такого сбоя складывается из возможности отказа, СУБД, сетевого оборудования, наличия необнаруженных ошибок в ПО. Поскольку время восстановления АИС при реализации перечисленных сбоев не более 5 дней, то риск возникновения экономических потерь можно оценить как незначительный (менее 1 %). Таким образом оценка риска 50000\*0,01=**500 руб.** |
| Потери времени на сомообучение и самостоятельное решение проблем | Отсутствуют |
| **Итого эксплуатационные расходы в год** | | **39 470 руб.** |

Затраты на разработку и внедрение составят примерно 475 тыс. руб., эксплуатационные расходы почти – 40 тыс.руб. в год.

**Шаг 4.** Оценка рисков позволит определить насколько полученные результаты могут стать меньше ожидаемого уровня. Каждый выделенный риск может потенциально сократить предполагаемые эффекты. Риски нужно формулировать как вероятность недополучения результатов, сформулированных как качественные показатели. При этом нужно разделять риски, имеющие влияние на один и тот же результат, по причинам их возникновения.

В соответствии с методикой REJ выделяют пять видов рисков. По каждому риску оценивается его влияние на результат и вероятность реализации по пятибалльной шкале.

Риск соответствия. Чем жестче соответствие ИТ-проекта целям предприятия, тем меньше риск. Необходимо заметить, что для некоторых проектов установление четкого соответствия технологий стратегическим целям бизнеса задача сложно выполнимая (например, усовершенствование инфраструктуры информационной системы), однако инвестиции в них являются необходимыми для дальнейшего развития информационных технологий.

Реализационный риск. Учитывает возможность того, что реальная стоимость реализации проекта будет отличаться от расчетной.

Операционный риск. Учитывает возможность того, что стоимость функционирования системы будет отличаться от предполагаемой.

Технологический риск. Чем больше известно о выбранном решении и чем проработанней выбранные технологии, тем меньше этот риск. Однако проекты с малым значением технологического риска не всегда обеспечивают достаточно высокие потенциальные преимущества. Как говорится: «Чем выше риск, тем выше прибыль».

Риск денежных потоков. Учитывает возможность недостоверного определения выгод от проекта и неточного расчета положительных денежных потоков, а также возможность появления других непредвиденных финансовых проблем. Например, будет принято решение увеличить капитализацию бизнеса или другие, более важные с точки зрения руководства, проблемы потребуют отвлечения средств от рассматриваемого проекта, в результате чего не удастся достичь предполагаемых выгод в полном объеме.

**Шаг 5.** Оценим показатели эффективности проекта. Ориентируясь на полученный на третьем шаге объем валовой прибыли можно оценить чистый приведенный доход. Первоначальные вложения - стоимость разработки и внедрения АИС – составляют 475 тыс.руб.; дополнительная прибыль примерно 240 тыс.руб. в год; дополнительные издержки (затраты на этапе эксплуатации) – 40 тыс. руб. в год; период (n) 3 года; ставка дисконтирования - для простоты используем ставку по коммерческим кредитам – 11,6%. Таким образом, чистый приведенный доход составит:

Внутренняя норма доходности проекта составит около 12,6%.

Срок окупаемости капитальных вложений составит: (475/200)\*12=2,4 года

Анализируя значения показателей, можно утверждать, что инвестирование средств в автоматизацию работы с дебиторской задолженностью будет целесообразным, т.к. чистый приведенный доход больше нуля, а срок окупаемости меньше, чем предполагаемый срок полезной эксплуатации

## Выводы по главе 3

Оценка экономической целесообразности работы.

Выбор программных и организационно–технологических проектных решений обеспечил минимизацию финансовых, материальных и трудовых затрат. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх.

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх.

Разработка является экономически целесообразной.

**Список использованных источников (ЭТО ДЛЯ ЭКОНОМИЧЕСКОГО РАЗДЕЛА, НО ВСТАВЛЯЕМ В ОБЩИЙ СПИСОК ЛИТЕРАТУРЫ)**

1. Анфилатов В.С. Системный анализ в управлении: учеб. Пособие/ В.С. Анфилатов, А.А. Емельянов, А.А. Кукушкин; под. ред. А.А. Емельянова.- М.: Финансы и статистика, 2007.-368 с.– 5/1/Э
2. Вендров А.М. Проектирование программного обеспечения экономических информационных систем: Учебник.-2-е изд., перераб и доп.- М.: Финансы и статистика, 2006.-544 с. 92/5/Э
3. Мишенин А.И. Теория экономических информационных систем: учебник, 4-е изд., доп и перераб..- М.: Финансы и статистика. 2007.-240с.: ил. 66/5/Э
4. Сатунина А.Е. Управление проектом корпоративной информационной системы предприятия: учеб. Пособие / А.Е. Сатунина, Л.А. Сысоева.- М.: Финансы и статистика; Инфра-М, 2009.-352с.: ил. 5/1/Э.
5. Системный анализ в менеджменте: электронный учебник / В.Н. Попов, В.С. Касьянов, И.П. Савченко. - Электрон. дан. - М.: КНОРУС, 2010/Э
6. Смирнова Г. Н. Проектирование экономических информационных систем : учеб. для эконом. вузов по специальностям "Прикладная информатика в экономике", "Прикладная информатика в менеджменте", "Прикладная информатика в юриспруденции" / Г. Н. Смирнова, А. А. Сорокин, Ю. Ф. Тельнов. - М. : Финансы и статистика, 2006. - 511 с. 58/5/Э
7. Теория систем и системный анализ в управлении организациями: Справочник: учеб. Пособие/ под ред. В.Н. Волковой и А.А. Емельянова.-М.: Финансы и статистика, 2006. - 848 с. 51/5/Э

# ЗАКЛЮЧЕНИЕ

В данной выпускной квалификационной работе, были выполнены поставленные задачи по проведению анализа предметной области организации работы электронной библиотеки в образовательном учреждении, были сформированы необходимые функциональные требования к разрабатываемой информационной системе, проведен подробный анализ баз данных и средств разработки, построена модель данных на физическом и логическом уровне, разработана корпоративная электронная библиотека ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх ххххххи дана экономическая оценка целесообразности разработки и ее себестоимости.

В результате выполнения задач, была Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх. согласно методологии “КАК ЕСТЬ” и ”КАК ДОЛЖНО БЫТЬ”.

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх.

По результатам был сделан расчет затрат на разработку корпоративной электронной библиотеки и сделан анализ экономической эффективности и целесообразности разработки и внедрения данного продукта.

# СПИСОК ЛИТЕРАТУРЫ

СПИСОК ЛИТЕРАТУРЫ ДОЛЖЕН БЫТЬ ОФОРМЛЕН ПО ГОСТ\_Р\_7\_0\_100\_2018

Можно воспользоваться ресурсом: https://perviy-vestnik.ru/literatura/?ysclid=lyfqldzbff465005388

1. Геворкян, Э. А. К теории распространения электромагнитных волн в волноводе с магнитоактивным анизотропным модулированным заполнением / Э. А. Геворкян // Радиотехника и электроника. – 2008. – Т. 53. – № 5. – С. 565-569. (ВОТ ЭТО ПРАВИЛЬНО!!!!)
2. Ресурс <http://www.mysql.ru/docs/>; (вот это **НЕ ПРАВИЛЬНО!!!! и ниже)**
3. Ресурс https://ru.wikipedia.org/wiki/;
4. Ресурс<https://www.php.net/manual/ru/language.functions.php>;
5. Ресурс <https://www.tadviser.ru/>;
6. Самоучитель PHP 7. Максим Кузнецов, Игорь Симдянов. изд. 2018;
7. HTML, JavaScript, PHP и MySQL. Джентльменский набор Web-мастера, 4-е издание,.Николай Прохоренок, Владимир Дронов., изд. 2015;
8. PHP и MySQL. Разработка веб-приложений, Денис Колисниченко., изд. 2017;
9. Милл А. Docker на практике, Сейерс Э. Х., изд. 2019;
10. Создание микросервисов, Ньюмен С. изд. 2016;
11. Информационные системы и технологии в экономике 3-е изд. Исправленное и дополненное, Нетёсова О. Ю. изд, 2019;
12. Компьютерные сети. Принципы, технологии, протоколы. Олифер Н.А., Олифер В.Г., изд. 2017;
13. Философия Java 4-е. Брюс Э. изд. 2019;
14. Структуры данных и алгоритмы в Java. Лафоре Р.,изд. 2018;
15. Базы данных. Практическое применение СУБД SQL и NoSOL-типа для применения проектирования информационных систем. Мартишин Сергей Анатольевич., изд. 2021;

# ПРИЛОЖЕНИЯ

## Приложение 1. Техническое задание на разработку корпоративной электронной библиотеки в университете

**ТЗ СТРОГО ПО ГОСТ 34.602-2020!!!!**

ГОСТ 34.602-2020. Межгосударственный стандарт. Информационные технологии. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы" (введен в действие Приказом Росстандарта от 19.11.2021 N 1522-ст)

ТЗ на АС является основным документом, определяющим требования и порядок создания автоматизированной системы, в соответствии с которым проводится разработка АС и ее приемка. ТЗ на другие виды работ (разработка, модернизация, развертывание, обновление отдельных модулей в составе АС и т.п.) также должно быть оформлено строго по ГОСТ 34.602-2020. При этом название вида работ отражается в наименовании ТЗ.

##### Общие сведения

В данном разделе указывают следующее:

- полное наименование АС и ее условное обозначение;

- шифр темы (при наличии);

- наименование организации - заказчика АС, наименование организации-разработчика (при наличии сведений о ней);

- перечень документов, на основании которых создается АС, кем и когда утверждены эти документы;

- плановые сроки начала и окончания работ по созданию АС;

- общие сведения об источниках и порядке финансирования работ

Хххххх хххх хххххххх хххххх, ххххххх ххххххх х ххххх хххххх ххххх. Ххх хх хх ххххххх хххххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххх ххххххххх хххххххххх ххххххххх ххххххх. Хх хххххххх хххххххххх хххххххх ххххххх ххххххххххх ххх ххххххх ххххххх ххххх хххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххххх хххх хххххххх хххххх, ххххххх ххххххх х ххххх хххххх ххххх. Ххх хх хх ххххххх хххххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххх ххххххххх хххххххххх ххххххххх ххххххх. Хх хххххххх хххххххххх хххххххх ххххххх ххххххххххх ххх ххххххх ххххххх ххххх хххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх.

Хххххх хххх хххххххх хххххх, ххххххх ххххххх х ххххх хххххх ххххх. Ххх хх хх ххххххх хххххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххх ххххххххх хххххххххх ххххххххх ххххххх. Хх хххххххх хххххххххх хххххххх ххххххх ххххххххххх ххх ххххххх ххххххх ххххх хххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх.

##### Цели и назначение создания автоматизированной системы

Раздел состоит из следующих подразделов:

- цели создания АС;

- назначение АС.

В подразделе "Цели создания АС" приводят наименования и требуемые значения технических, технологических, производственно-экономических или других показателей объекта автоматизации, которые должны быть достигнуты в результате создания АС, и указывают критерии оценки достижения целей создания АС.

В подразделе "Назначение АС" указывают вид автоматизируемой деятельности (управление, проектирование и т.п.) применительно к объекту автоматизации в целом.

Хххххх хххх хххххххх хххххх, ххххххх ххххххх х ххххх хххххх ххххх. Ххх хх хх ххххххх хххххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххх ххххххххх хххххххххх ххххххххх ххххххх. Хх хххххххх хххххххххх хххххххх ххххххх ххххххххххх ххх ххххххх ххххххх ххххх хххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх.

##### Характеристика объектов автоматизации

В этом разделе приводят следующую информацию:

- основные сведения об объекте автоматизации или ссылки на документы, содержащие такие сведения;

- сведения об условиях эксплуатации объекта автоматизации и характеристиках окружающей среды.

Хххххх хххх хххххххх хххххх, ххххххх ххххххх х ххххх хххххх ххххх. Ххх хх хх ххххххх хххххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххх ххххххххх хххххххххх ххххххххх ххххххх. Хх хххххххх хххххххххх хххххххх ххххххх ххххххххххх ххх ххххххх ххххххх ххххх хххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх.

##### Требования к автоматизированной системе

Раздел состоит из следующих подразделов:

- требования к структуре АС в целом;

- требования к функциям (задачам), выполняемым АС;

- требования к видам обеспечения АС;

- общие технические требования к АС.

Состав требований к АС, включаемых в данный раздел ТЗ на АС, устанавливают в зависимости от вида, назначения, специфических особенностей и условий функционирования конкретной автоматизированной системы. В каждом подразделе приводят ссылки на действующие НТД, определяющие требования к автоматизированным системам соответствующего вида.

Хххххх хххх хххххххх хххххх, ххххххх ххххххх х ххххх хххххх ххххх. Ххх хх хх ххххххх хххххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххх ххххххххх хххххххххх ххххххххх ххххххх. Хх хххххххх хххххххххх хххххххх ххххххх ххххххххххх ххх ххххххх ххххххх ххххх хххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх.

##### Состав и содержание работ по созданию автоматизированной системы

Раздел должен содержать перечень этапов работ по созданию АС и сроки их выполнения. Хххххх хххх хххххххх хххххх, ххххххх ххххххх х ххххх хххххх ххххх. Ххх хх хх ххххххх хххххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххх ххххххххх хххххххххх ххххххххх ххххххх. Хх хххххххх хххххххххх хххххххх ххххххх ххххххххххх ххх ххххххх ххххххх ххххх хххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх.

##### Порядок разработки автоматизированной системы

В разделе приводят следующее:

- порядок организации разработки АС;

- перечень документов и исходных данных для разработки АС;

- перечень документов, предъявляемых по окончании соответствующих этапов работ;

- порядок проведения экспертизы технической документации;

- перечень макетов (при необходимости), порядок их разработки, изготовления, испытаний, необходимость разработки на них документации, программы и методик испытаний;

- порядок разработки, согласования и утверждения плана совместных работ по разработке АС;

- порядок разработки, согласования и утверждения программы работ по стандартизации;

- требования к гарантийным обязательствам разработчика;

- порядок проведения технико-экономической оценки разработки АС;

- порядок разработки, согласования и утверждения программы метрологического обеспечения, программы обеспечения надежности, программы эргономического обеспечения.

Хххххх хххх хххххххх хххххх, ххххххх ххххххх х ххххх хххххх ххххх. Ххх хх хх ххххххх хххххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххх ххххххххх хххххххххх ххххххххх ххххххх. Хх хххххххх хххххххххх хххххххх ххххххх ххххххххххх ххх ххххххх ххххххх ххххх хххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх.

##### Порядок контроля и приемки автоматизированной системы

В разделе указывают следующую информацию:

- виды, состав и методы испытаний АС и ее составных частей;

- общие требования к приемке работ, порядок согласования и утверждения приемочной документации;

- статус приемочной комиссии (государственная, межведомственная, ведомственная и др.)

Хххххх хххх хххххххх хххххх, ххххххх ххххххх х ххххх хххххх ххххх. Ххх хх хх ххххххх хххххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххх ххххххххх хххххххххх ххххххххх ххххххх. Хх хххххххх хххххххххх хххххххх ххххххх ххххххххххх ххх ххххххх ххххххх ххххх хххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх.

##### Требования к составу и содержанию работ по подготовке объекта автоматизации к вводу автоматизированной системы в действие

В разделе приводят перечень мероприятий, которые необходимо осуществить при подготовке объекта автоматизации к вводу АС в действие.

В перечень мероприятий включают следующее:

- создание условий функционирования объекта автоматизации, при которых гарантируется соответствие создаваемой АС требованиям, содержащимся в ТЗ на АС;

- проведение необходимых организационно-штатных мероприятий;

- порядок обучения персонала и пользователей АС

Хххххх хххх хххххххх хххххх, ххххххх ххххххх х ххххх хххххх ххххх. Ххх хх хх ххххххх хххххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххх ххххххххх хххххххххх ххххххххх ххххххх. Хх хххххххх хххххххххх хххххххх ххххххх ххххххххххх ххх ххххххх ххххххх ххххх хххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх.

##### Требования к документированию

В разделе приводят следующую информацию:

- перечень подлежащих разработке документов;

- вид представления и количество документов;

- требования по использованию ЕСКД и ЕСПД при разработке документов.

При отсутствии государственных стандартов, определяющих требования к документированию элементов АС, дополнительно включают требования к составу и содержанию таких документов.

Хххххх хххх хххххххх хххххх, ххххххх ххххххх х ххххх хххххх ххххх. Ххх хх хх ххххххх хххххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххх ххххххххх хххххххххх ххххххххх ххххххх. Хх хххххххх хххххххххх хххххххх ххххххх ххххххххххх ххх ххххххх ххххххх ххххх хххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх.

##### Источники разработки

В разделе "Источники разработки" должны быть перечислены документы и информационные материалы (технико-экономическое обоснование, отчеты о законченных научно-исследовательских работах, информационные материалы на отечественные, зарубежные системы-аналоги и др.), на основании которых разрабатывалось ТЗ и которые должны быть использованы при создании АС.

Хххххх хххх хххххххх хххххх, ххххххх ххххххх х ххххх хххххх ххххх. Ххх хх хх ххххххх хххххххх ххххххх. Ххххх ххххххххххх хххххх, хххххх, ххххххххххх хххххх хххххххх ххх хххххххх хххххххх хххххххх ххххх. Хххх ххххххххх хххххххххх ххххххххх ххххххх. Хх хххххххх хххххххххх хххххххх ххххххх ххххххххххх ххх ххххххх ххххххх ххххх хххххх ххххххх. Ххххх

## Приложение 2. Исходный код “Авторизация”

<!--Проверка авторизован ли пользователь-->

<?php

session\_start - );

if - isset - $\_SESSION['uid']) & isset - $\_SESSION['nm']))

{

$id = $\_SESSION['uid'];

$redir = "Location: $id"."prof.php";

header - "$redir");

exit - );

}

?>

<!--Стили блоков-->

<style type="text/css">

.buttons

{

background-color: #FF0000;

width: 110px;

height: 25px;

cursor: pointer;

color: #FFFFFF;

}

</style>

<!--Стиль блока авторизации-->

<style type="text/css">

.loginstyle

{

background-color: #CACACA;

position: absolute;

left: 39%;

top: 35%;

color: #000000;

border:5px;

border-spacing: 3px 10px;

border: 3px solid;

}

</style>

<!--Стиль тела сайта-->

<style type="text/css">

body

{

background:url - logos/mainlog.jpg) fixed no-repeat center;

background-size: 100%;

-moz-background-size: 100%; /\* Firefox 3.6+ \*/

-webkit-background-size: 100%; /\* Safari 3.1+ и Chrome 4.0+ \*/

-o-background-size: 100%; /\* Opera 9.6+ \*/

}

</style>

<!--Стиль нижнего блока-->

<style type="text/css">

.nblock

{

position: fixed;

bottom:0;

color: #FFFFFF;

border: 2px solid;

background-color: #FF4500;

width: 100%;

}

</style>

<!--HTML структура-->

<html>

<head>

<title>Вход в систему учета заявок "RTSuppService"</title>

</head>

<body>

<form method="post">

<table class="loginstyle" width="400" height="250">

<tr><td></td></tr>

<tr><td><b><p align="center">Ваш логин:</p></b></td></tr>

<tr><td><p align="center"><input type="text" name="login" maxlength="15" pattern="[A-Za-z-0-9]{4,15}" style="width:140"></p></td></tr>

<tr><td><b><p align="center">Ваш пароль:</p></b></td></tr>

<tr><td><p align="center"><input type="password" name="pass" maxlength="15" pattern="[A-Za-z-0-9]{4,15}" style="width:140"></p></td></tr>

<tr><td><p align="center"><input class="buttons" type="submit" value="Войти">&nbsp &nbsp <input class="buttons" type="submit" formaction="reg.php" value="Информация"></p></td></tr>

</table>

</form>

</body>

<table class="nblock">

<tr><td><p align="center">RTSuppService Rostelecom's CRM system Москва 2020г.</p></td></tr>

</table>

</html>

<!--PHP скрипт,обработка форм-->

<?php

//Проверка существования переменной

if - isset - $\_POST['login']) && isset - $\_POST['pass']))

{

$login = $\_POST['login'];

$pass = $\_POST['pass'];

//Проверка на пустое поле

if - !empty - $login && $pass))

{

//sql запросы в БД

$link = mysqli\_connect - "localhost","root","9522687799");

mysqli\_select\_db - $link,'usrid');

$query = mysqli\_query - $link,"select uid,uname,usurname,firstname,upass,ugroup from sp\_users WHERE ulogin='".mysqli\_real\_escape\_string - $link,$\_POST['login'])."' LIMIT 1");

$data = mysqli\_fetch\_assoc - $query);

if - $data['upass'] == $\_POST['pass'])

{

if - !isset - $\_SESSION['login']))

{

session\_start - );

$nm = $data['uname'];

$usur = $data['usurname'];

$fnm = $data['firstname'];

$uid = $data['uid'];

$group = $data['ugroup'];

$\_SESSION['nm'] = $nm;

$\_SESSION['usurname'] = $usur;

$\_SESSION['firstname'] = $fnm;

$\_SESSION['uid'] = $uid;

$\_SESSION['ugroup'] = $group;

$profilenm = "Location: $uid"."prof.php";

header - "$profilenm");

}

}

else

{

//echo "<br><br><br><br><br><br><p align=center><img src=smiles/grust.gif><br></p>";

}

}

else

{

//echo "<br><br><br><br><br><p align=center><img src=smiles/vvod.gif></p>";

return;

}

}

?>

## Приложение 3. Руководство администратора корпоративной информационной системы

Для дальнейшей эксплуатации информационной системы, необходимо составить сопроводительный документ – “руководство администратора”.

Сама структура и все необходимые требования к содержанию руководства пользователя по ГОСТ 34, описаны в РД 50-34.698-90.

В руководстве администратора отражаем АДМИНИСТРИРОВАНИЕ СИСТЕМЫ! Сюда относится – установка и развертывание ПО, интеграция с существующими системами, настройка системных файлов, настройка прав доступа

##### Введение

В разделе "Введение" указывают:

1) область применения;

2) краткое описание возможностей;

3) уровень подготовки пользователя;

4) перечень эксплуатационной документации, с которой необходимо ознакомиться пользователю

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх.

##### Назначение и условия применения

В разделе "Назначение и условия применения" указывают:

1) виды деятельности, функции, для автоматизации которых предназначено данное средство автоматизации;

2) условия, при соблюдении (выполнении, наступлении) которых обеспечивается применение средства автоматизации в соответствии с назначением (например, вид ЭВМ и конфигурация технических средств, операционная среда и общесистемные программные средства, входная информация, носители данных, база данных, требования к подготовке специалистов и т.п.)

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх.

##### Подготовка к работе

В разделе "Подготовка к работе" указывают:

1) состав и содержание дистрибутивного носителя данных;

2) порядок загрузки данных и программ;

3) порядок проверки работоспособности.

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх.,

##### Описание операций

В разделе "Описание операций" указывают:

1) описание всех выполняемых функций, задач, комплексов задач, процедур;

2) описание операций технологического процесса обработки данных, необходимых для выполнения функций, комплексов задач (задач), процедур.

Для каждой операции обработки данных указывают:

1) наименование;

2) условия, при соблюдении которых возможно выполнение операции;

3) подготовительные действия;

4) основные действия в требуемой последовательности;

5) заключительные действия;

6) ресурсы, расходуемые на операцию.

В описании действий допускаются ссылки на файлы подсказок, размещенные на магнитных носителях.

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх.

##### Аварийные ситуации

В разделе "Аварийные ситуации" указывают:

1) действия в случае несоблюдения условий выполнения технологического процесса, в том числе при длительных отказах технических средств;

2) действия по восстановлению программ и (или) данных при отказе магнитных носителей или обнаружении ошибок в данных;

3) действия в случаях обнаружения несанкционированного вмешательства в данные;

4) действия в других аварийных ситуациях

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх.

##### Рекомендации по освоению

В разделе "Рекомендации по освоению" указывают рекомендации по освоению и эксплуатации, включая описание контрольного примера, правила его запуска и выполнения

Ххххх ххххххх хххххх хххххх ххххххх ххххххх ххххх ххх ххххх. Хххх ххххх ххххх хххххххх хххх хххх хх ххххххх хххххххх хх х х ххххххх. Ххх ххх ххххххх ххххххх ххххххх ххххххх ххххх хххххххххх ххххххх ххххххххх хххххх.

## Приложение 4. Политика информационной безопасности ЭТО ПРИМЕР! НЕ НУЖНО ВСЕ СЕБЕ КОПИРОВАТЬ!!

##### ОБЩИЕ ПОЛОЖЕНИЯ

* 1. Настоящая политика информационной безопасности (далее - Политика) утверждается руководителем {Название Организации} и определяет мероприятия, процедуры и правила по защите информации в информационных системах {Название Организации}.
  2. Положения настоящей Политики распространяются на следующие информационные системы {Название Организации}:
* ГИС «ИС»;
* ИСПДн «Бухгалтерия и кадры»;
* ИС «Делопроизводство».
  1. Положения настоящей Политики обязательны к исполнению для всех пользователей указанных в п. 1.2 информационных систем (далее - Пользователи), а также для администраторов безопасности и системных администраторов (далее - Администраторы).
  2. В соответствии с указом Президента Российской Федерации № 188 от 6 марта 1997 года к сведениям конфиденциального характера (защищаемой информации) в {Название Организации} относятся:
* сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;
* сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее) {оставить нужное};
* служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна) {только для госов};
* сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).
  1. Целями настоящей Политики являются:
* обеспечение конфиденциальности, целостности, доступности защищаемой информации;
* предотвращение утечек защищаемой информации;
* мониторинг событий безопасности и реагирование на инциденты безопасности;
* нейтрализация актуальных угроз безопасности информации;
* выполнение требований действующего законодательства по защите информации.
  1. В настоящей Политике используются термины и определения, установленные законодательством Российской Федерации об информации, информационных технологиях и о защите информации, а также термины и определения, установленные национальными стандартами в области защиты информации.
  2. Настоящая Политика разработана с учетом положений следующих законодательных и нормативно-правовых актов:
* Федеральный закон № 149-ФЗ от 27 июля 2006 года «Об информации, информатизации и защите информации»;
* Федеральный закон № 152-ФЗ от 27 июля 2006 года «О персональных данных»;
* «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные Постановлением Правительства РФ № 1119 от 1 ноября 2012 года;
* «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России № 17 от 11 февраля 2013 года;
* «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденный приказом ФСТЭК России № 21 от 18 февраля 2013 года;
* методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014 года;
* «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», утверждённые приказом ФСБ России № 378 от 10.07.2014;
* «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», утвержденное приказом ФСБ от 9 февраля 2005 №66;
* «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная приказом ФАПСИ от 13 июня 2001 №152.

##### ТЕХНОЛОГИЧЕСКИЕ ПРОЦЕССЫ ОБРАБОТКИ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

* 1. В данном разделе настоящей Политики описаны технологические процессы обработки различных видов защищаемой информации в информационных системах {Название Организации}. Администраторы и Пользователи, допущенные к обработке той или иной защищаемой информации, обязаны производить обработку этой информации в соответствии с соответствующими описаниями технологических процессов обработки информации, приведенных в данном разделе.
  2. Технологический процесс обработки персональных данных сотрудников {Название Организации}:

{описать техпроцесс}

* 1. Технологический процесс обработки персональных данных соискателей на вакантные должности в {Название Организации}:

{описать техпроцесс}

* 1. Технологический процесс обработки персональных данных клиентов на вакантные должности в {Название Организации}:

{описать техпроцесс}

##### ПРАВИЛА И ПРОЦЕДУРЫ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ГИС, ПОЛИТИКА РАЗГРАНИЧЕНИЯ ДОСТУПА К РЕСУРСАМ ГИС

* 1. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику {Название Организации}, допущенному к работе с ресурсами ГИС «Бухгалтерия и кадры» присваивается уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в ГИС.
  2. Под учетной записью Пользователя понимается учетная запись для доступа к информационной системе в домене Active Directory. Если применяется дополнительное разграничение доступа, например в 1С, дописать это.
  3. Использование одного и того же имени пользователя несколькими пользователями (или группового имени для нескольких пользователей) в ГИС запрещено.
  4. Для администратора безопасности ГИС, для системных администраторов ГИС, для удаленных пользователей (пользователей работающих с ресурсами ГИС через внешние телекоммуникационные сети, но являющихся сотрудниками {Название Организации}), для внешних пользователей ГИС (пользователей, не являющихся сотрудниками ГИС) предусмотрена двухфакторная аутентификация в ГИС. (для ГИС К1: Для всех пользователей ГИС (в том числе для внешних пользователей и удаленных пользователей) предусмотрена двухфакторная аутентификация) Двухфакторная аутентификация подразумевает под собой обязательное выполнение двух факторов: предъявление физического электронного ключа eToken PRO Java 72K (JaCarta, RuToken и тд), и ввод пароля (пин-кода) доступа к памяти электронного ключа. Электронные ключи и пароли доступа выдаются Администратором в соответствии с теми же требованиями и правилами, установленными для выдачи учетных записей и паролей к ним в данном разделе настоящей Политики. Идентификация электронного ключа и считывание аутентификационной информации с него осуществляется с помощью механизмов средства защиты информации от несанкционированного доступа (далее - СЗИ от НСД) {Название СЗИ от НСД}.
  5. Процедура регистрации (создания учетной записи и выдачи при необходимости электронного ключа) пользователя ГИС для сотрудника {Название Организации}, и предоставления ему (или изменения его) прав доступа к ресурсам ГИС инициируется заявкой руководителя подразделения, в котором работает этот сотрудник. Форма заявки приведена в Приложении № 1 к настоящей Политике. В заявке указывается:
* содержание запрашиваемых изменений (регистрация нового пользователя ГИС, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам ГИС ранее зарегистрированного пользователя);
* должность (с полным наименованием подразделения), фамилия, имя и отчество сотрудника;
* полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач в ГИС);
* заявку визирует администратор безопасности, утверждая тем самым возможность допуска (изменения прав доступа) данного сотрудника к необходимым для решения им указанных задач ресурсам ГИС.
  1. Администратор перед визированием заявки осуществляет верификацию пользователя (подтверждает его личность), а также уточняет его должностные и функциональные обязанности и сопоставляет их с технологическими процессами обработки информации, описанным в разделе 2 настоящей Политики. Допуск Пользователей к обработке информации в ГИС производится на основании завизированной Администратором заявки, составленной по форме, приведенной в Приложении № 1 к настоящей Политике. При визировании очередной заявки Администратор осуществляет актуализацию следующих документов:
* положение о разграничении прав доступа в ГИС (при необходимости, Приложение № 2 к настоящей Политике);
* Перечень лиц, должностей, служб и процессов, допущенных к работе с ресурсами ГИС «Бухгалтерия и кадры» (Приложение № 3 к настоящей Политике).
  1. После визирования заявки Администратор определяет тип учетной записи (внутренний пользователь, внешний пользователь, системная, учетная запись приложения, временная, гостевая) и производит необходимые настройки СЗИ от НСД и формирует учетную запись, персональный идентификатор и первичный пароль. Дает ознакомиться с инструкцией Пользователя ГИС под роспись, сообщает пользователю идентификационные данные и допускает к работе в ГИС. После допуска к работе в ГИС, Пользователь самостоятельно формирует пароль доступа к своей учетной записи в соответствии с требованиями раздела 3 Инструкции Пользователя ГИС.
  2. {К1} В ГИС «Бухгалтерия и кадры» для учетных записей Пользователей, процессов, приложений, гостевых и временных учетных записей разрешен только один параллельный сеанс доступа к ресурсам ГИС. Для привилегированных учетных записей (администратор безопасности и системные администраторы) разрешено не более двух параллельных сеансов доступа к ресурсам ГИС с разных устройств. Настройка разрешения параллельных сеансов доступа к ресурсам ГИС осуществляется Администратором путем указания соответствующих параметров в {Название СЗИ от НСД}. Контроль и отображение числа активных одновременных (параллельных) сеансов доступа для каждой учетной записи осуществляется во вкладке «Сессии» сервера безопасности Dallas Lock 8.0-K.
  3. По окончании внесения изменений в списки пользователей в заявке делается отметка о выполнении задания. Исполненная заявка хранится у Администратора и может быть использована для восстановления полномочий пользователей после сбоев в работе ГИС, а также для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам ГИС при разборе инцидентов безопасности.
  4. Для проведения временных работ в ГИС сотрудниками сторонних организаций предусмотрена гостевая временная учетная запись «Guest». Данная учетная запись отключена и активируется (наделяется необходимыми полномочиями) только при необходимости. Все работы от имени такой учетной записи проводятся только под контролем Администратора.
  5. В качестве модели разграничения доступа к ресурсам ГИС выбрана ролевая модель. Пользователям назначается роль в разграничительной системе ГИС в зависимости от выполняемых должностных обязанностей и задач и, соответственно, в зависимости от необходимости по доступу к тем или иным ресурсам ГИС. Обязанности и задачи пользователей определяются исходя из технологических процессов обработки информации, описанных в разделе 2 настоящей Политики. Описание всех возможных ролей в ГИС приведено в Приложении № 2 к настоящей Политике. Помимо учетных записей Пользователей доступ к системе получают различные системные службы и процессы.
  6. Перечень лиц, их должностей, а также служб и процессов, допущенных к работе с ресурсами ГИС и сопоставляемые им роли приведены в Приложении № 3 к настоящей Политике. Администратор обеспечивает оперативное обновление и актуальность данного перечня.
  7. Перечень помещений, в которых разрешена работа с ресурсами ГИС, расположены технические средства ГИС, а также перечень лиц, допущенных в эти помещения приведен в Приложении № 4 к настоящей Политике. Администратор обеспечивает оперативное обновление и актуальность данного перечня.
  8. {К2+} Перечень устройств (стационарных, мобильных, портативных), используемых в ГИС приведен в приложении № 4 к настоящей Политике. Администратор обеспечивает оперативное обновление и актуальность данного перечня. Идентификация и аутентификация устройств в ГИС осуществляется по совокупности имени или ID устройства, IP-адреса {убрать, если динамика} и MAC-адреса. Идентификация и аутентификация устройств осуществляется с помощью механизмов СЗИ от НСД {Название СЗИ от НСД}. В случае выявления посторонних устройств, Администратор оперативно блокирует доступ неустановленного устройства к ГИС и созывает ГРИИБ, которая в свою очередь устанавливает причины и последствия такого инцидента.
  9. Идентификация и аутентификация на сетевом оборудовании (коммутаторы, маршрутизаторы, точки доступа и т. д.) разрешена только администраторам безопасности, системным администраторам и сотрудникам сторонней организации, производящим работы в сети {Название Организации} на договорной основе под контролем Администратора. При вводе в эксплуатацию сетевого оборудования на нем обязательно меняются идентификационные и аутентификационные данные, установленные производителем устройства по умолчанию. Новые идентификационные данные на сетевых устройствах должны соответствовать установленной парольной политике.
  10. Пользователям запрещены любые действия в ГИС до прохождения процедуры идентификации и аутентификации в системе. Администратору разрешается ряд действий до прохождения идентификации и аутентификации в ГИС в ряде случаев. Условия, при которых разрешаются такие действия и перечень разрешенных действий для Администратора до прохождения процедуры идентификации и аутентификации в ГИС перечислены в пункте 5.9 инструкции Администратора.

##### ПРАВИЛА И ПРОЦЕДУРЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ ПОТОКАМИ

* 1. {Описать}

##### ПРАВИЛА И ПРОЦЕДУРЫ УПРАВЛЕНИЯ УСТАНОВКОЙ (ИНСТАЛЯЦИЕЙ) КОМПОНЕНТОВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

* 1. В ГИС «Бухгалтерия и кадры» разрешено использование только того программного обеспечения, его компонентов, утилит и драйверов, которые необходимы для обеспечения функционирования информационной системы, а также необходимы для выполнения служебных (должностных) обязанностей пользователями.
  2. Перечень разрешенного программного обеспечения в ГИС «Бухгалтерия и кадры» определен в Приложении № 7 к настоящей Политике.
  3. Установка программного обеспечения, его компонент, утилит и драйверов осуществляется только системными администраторами или администратором безопасности в соответствии с Приложением № 7. Пользователям запрещена установка любого ПО в ГИС «Бухгалтерия и кадры».
  4. Пользователь имеет право подать заявку в виде служебной записки на включение в список разрешенного в ГИС программного обеспечения, необходимых ему для выполнения служебных (должностных) обязанностей программ, утилит, драйверов. В такой служебной записке обязательно указывается обоснование необходимости включения в этот список нового программного обеспечения. Срок рассмотрения заявки должен составлять не более 3 рабочих дней.
  5. Администратор ежемесячно с помощью инструмента XSpider 7.8.24 проводит проверку соответствия состава программного обеспечения в ГИС «Бухгалтерия и кадры» списку разрешенного ПО. В случае выявления постороннего программного обеспечения, созывается группа реагирования на инциденты информационной безопасности, которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.
  6. {К1} На серверной части ГИС «Бухгалтерия и кадры» при загрузке операционных систем серверов запускается следующее программное обеспечение:
* MS SQL Server;
* IIS;
* ...
  1. {К1} На АРМ Пользователей ГИС «Бухгалтерия и кадры» при загрузке операционных систем серверов запускается следующее программное обеспечение:
* MS SQL Server;
* IIS;
* ...
  1. {К1} На АРМ Администратора ГИС «Бухгалтерия и кадры» при загрузке операционных систем серверов запускается следующее программное обеспечение:
* MS SQL Server;
* IIS;
* ...

##### ЗАЩИТА МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ, КОНТРОЛЬ ИНТЕРФЕЙСОВ ВВОДА-ВЫВОДА, ГАРАНТИРОВАННОЕ УНИЧТОЖЕНИЕ ИНФОРМАЦИИ

* 1. {Описать}

##### РЕГЛАМЕНТАЦИЯ И КОНТРОЛЬ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ БЕСПРОВОДНОГО ДОСТУПА И ЗАЩИТА БЕСПРОВОДНЫХ СОЕДИНЕНИЙ {Удалить раздел, если нет беспроводных соединений}

* 1. {Описать}

##### УПРАВЛЕНИЕ ВЗАИМОДЕЙСТВИЕМ С ИНФОРМАЦИОННЫМИ СИСТЕМАМИ СТОРОННИХ ОРГАНИЗАЦИЙ (ВНЕШНИМИ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ) {Удалить раздел, если нет такого взаимодействия}

* 1. {Описать}

##### ПРАВИЛА И ПРОЦЕДУРЫ ОБЕСПЕЧЕНИЯ ДОВЕРЕННОЙ ЗАГРУЗКИ СРЕДСТВ ВЫЧИСЛИТЕЛЬНО ТЕХНИКИ {К2+}

* 1. В {Название Организации} в качестве средства доверенной загрузки технических средств применяется {Название МДЗ}. {Убрать, если применяются компенсирующие меры}
  2. Для работы с ресурсами ГИС «Бухгалтерия и кадры» выбираются такие технические средства, базовая система ввода-вывода которых (BIOS/UEFI) позволяет отключить возможность выбора источника загрузки в обход настроек BIOS/UEFI (вызов вариантов источников загрузки одной из функциональных клавиш).
  3. Администратор контролирует работоспособность {Название МДЗ} в соответствии с планом периодических мероприятий по контролю защищенности информации. По результатам проверки делается запись в журнал периодического тестирования средств защиты информации. {Убрать, если применяются компенсирующие меры}
  4. В случае некорректной работы средства доверенной загрузки на техническом средстве, такое техническое средство изымается из ГИС на время проведения ремонта/замены средства доверенной загрузки. В случае необходимости продолжения работы на техническом средстве, применяются следующие компенсирующие меры {Убрать, если применяются компенсирующие меры}:
* опечатываются USB-порты, входы для SD/Micro-SD и других карт памяти, CD/DVD/Blu-Ray-приводы и сами технические средства;
* устанавливается пароль администратора на вход в BIOS/UEFI и отключается возможность вызова источника загрузки нажатием функциональной клавиши (F1-F12) при загрузке;
* устанавливается усиленный визуальный контроль за техническим средством.
  1. В проектной документации на систему защиты информации в ГИС «Бухгалтерия и кадры» обосновано применение компенсирующих мер, нейтрализующих угрозы безопасности информации, связанные с недоверенной загрузкой технических средств ГИС. {Убрать, если применяется МДЗ}
  2. В качестве компенсирующей меры в ГИС «Бухгалтерия и кадры» применяется опечатывание USB-портов, входов для SD/Micro-SD и других карт памяти, CD/DVD/Blu-Ray-приводов и самих технических средств. Данная мера обеспечивает контроль доступа злоумышленника к интерфейсам ввода-вывода, позволяющим осуществить недоверенную загрузку. {Убрать, если применяется МДЗ}
  3. В качестве компенсирующей меры в ГИС «Бухгалтерия и кадры» применяется установка пароля администратора на вход в BIOS/UEFI и отключение возможности вызова источника загрузки во время загрузки технического средства. Данная мера позволяет блокировать на программном уровне изменение источника загрузки при срыве пломбы с интерфейса ввода-вывода. {Убрать, если применяется МДЗ}
  4. В качестве компенсирующей меры в ГИС «Бухгалтерия и кадры» применяется усиленный визуальный контроль за техническими средствами ГИС. Данная мера позволяет своевременно детектировать факты нарушения пломб технического средства, выявлять факты несанкционированного доступа и принимать меры реагирования. {Убрать, если применяется МДЗ}
  5. Администратор контролирует выполнение компенсирующих мер в соответствии с планом периодических мероприятий по контролю защищенности информации. По результатам проверки делается запись в журнал периодического тестирования средств защиты информации. {Убрать, если применяется МДЗ}

##### ПРАВИЛА И ПРОЦЕДУРЫ ПРИМЕНЕНИЯ УДАЛЕННОГО ДОСТУПА {Убрать раздел, если нет удаленного доступа}

* 1. {Описать}

##### ПРАВИЛА И ПРОЦЕДУРЫ ОБНАРУЖЕНИЯ (ПРЕДОТВРАЩЕНИЯ) ВТОРЖЕНИЙ {К2+}

* 1. {Описать}

##### ПРАВИЛА И ПРОЦЕДУРЫ ВЫЯВЛЕНИЯ, АНАЛИЗА И УСТРАНЕНИЯ УЯЗВИМОСТЕЙ

* 1. В {Название Организации} в качестве средства выявления уязвимостей используется сертифицированный сканер уязвимостей {название сканера}.
  2. Администратор не реже одного раза в месяц проводит полное сканирование системы на выявление уязвимостей. В случае поступления информации из новостных источников об уязвимостях в операционных системах и/или прикладном программном обеспечении применяемых в ГИС «Бухгалтерия и кадры» производится внеплановое обновление базы данных сканера уязвимостей и полное сканирование информационной системы.
  3. Администратор изучает отчеты по результатам сканирования и принимает решение о немедленном устранении выявленных уязвимостей, либо о включении мероприятий по устранению выявленных уязвимостей в план мероприятий по защите информации, в случае если выявленные уязвимости не являются критичными, или если есть возможность сделать невозможным их эксплуатацию потенциальным злоумышленником (например, путем отключения отдельных АРМ и/или сегментов сети от Интернет). При необходимости, для адекватного реагирования на вновь выявленные угрозы может созываться ГРИИБ.
  4. Критичность уязвимостей может быть установлена как на основании рейтинга уязвимости по шкале CVSS, так и на основании оценки рисков информационной безопасности в соответствии с ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».
  5. При выявлении уязвимостей, Администратор анализирует системные журналы и журналы средств защиты информации, на предмет выявления эксплуатации выявленной уязвимости в информационной системе и последствий такой эксплуатации.
  6. В случае невозможности оперативного устранения критичной уязвимости, Администратор уведомляет об этом руководителя {Название Организации}.

##### ПРАВИЛА И ПРОЦЕДУРЫ КОНТРОЛЯ УСТАНОВКИ ОБНОВЛЕНИЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

* 1. {Описать}

##### ПРАВИЛА И ПРОЦЕДУРЫ КОНТРОЛЯ СОСТАВА ТЕХНИЧЕСКИХ СРЕДСТВ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

* 1. Состав технических средств (далее – ТС), программного обеспечения (далее – ПО) и средств защиты информации (далее – СрЗИ) ГИС «Бухгалтерия и кадры» фиксируется в техническом паспорте на информационную систему. Технический паспорт является эталоном состава ТС, ПО и СрЗИ, по которому осуществляется периодический контроль.
  2. В случае добавления новых ТС, ПО и СрЗИ в состав ГИС «Бухгалтерия и кадры» или удаления существующих компонентов, на основании акта ввода в эксплуатацию (или акта вывода из эксплуатации) максимально оперативно вносятся изменения в Технический паспорт.
  3. Администратор осуществляет контроль состава ТС, ПО и СрЗИ не реже одного раза в месяц.
  4. Выявление несоответствия состава ТС, ПО и СрЗИ техническому паспорту ГИС «Бухгалтерия и кадры» является инцидентом безопасности. В случае выявления фактов несоответствия Администратор устанавливает причины самостоятельно или созывает ГРИИБ.
  5. В случае выявления несоответствия состава ТС, ПО и СрЗИ, Администратор принимает меры по оперативному исключению (восстановлению) из состава (в составе) информационной системы несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.
  6. Администратор осуществляет контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принимает меры, направленные на устранение выявленных недостатков. В случае, если сертификат соответствия истек, но был продлен производителем СрЗИ, Администратор запрашивает актуальную заверенную копию сертификата. В случае, если сертификат соответствия истек, но не был продлен производителем СрЗИ, то Администратор сообщает об этом руководителю {Название Организации}, который принимает решение об организации самостоятельной сертификации использующегося СрЗИ, либо об обновлении использующегося СрЗИ до актуальной версии, либо о замене использующегося СрЗИ на другое аналогичное сертифицированное СрЗИ.

##### {К2+} ПРАВИЛА И ПРОЦЕДУРЫ КОНТРОЛЯ ЦЕЛОСТНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

* 1. {Описать}

##### ПРАВИЛА И ПРОЦЕДУРЫ РЕЗЕРВИРОВАНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, БАЗ ДАННЫХ, СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ И ИХ ВОССТАНОВЛЕНИЯ ПРИ ВОЗНИКНОВЕНИИ НЕШТАТНЫХ СИТУАЦИЙ

* 1. Резервирование информационных ресурсов (программного обеспечения, баз данных, средств защиты информации) ГИС «Бухгалтерия и кадры» осуществляется в соответствии с инструкцией администратора безопасности информации и в соответствии с Приложением № 10 к настоящей Политике.
  2. {К2+} Администратор осуществляет с периодичностью, установленной в плане мероприятий по обеспечению режима защиты информации проверку работоспособности средств резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий. По результатам проверки делается запись в журнале учета мероприятий по контролю за соблюдением режима защиты информации. В случае выявления проблем с системой резервирования, принимаются меры по восстановлению ее работоспособности. После восстановления работоспособности системы резервирования осуществляется внеплановое резервное копирование всех информационных ресурсов ГИС «Бухгалтерия и кадры».
  3. Резервирование технических средств осуществляется в соответствии с проектной документацией (эскизным проектом) на систему защиты информации ГИС «Бухгалтерия и кадры».
  4. Восстановление из резервных копий является основным методом восстановления работоспособности информационной системы после ликвидации нештатных ситуаций.
  5. Нештатными ситуациями являются:
* разглашение информации ограниченного доступа сотрудниками {Название Организации}, имеющими к ней право доступа, в том числе:
  + разглашение информации лицам, не имеющим права доступа к защищаемой информации;
  + передача информации по незащищенным каналам связи;
  + обработка информации на незащищенных технических средствах обработки информации;
  + опубликование информации в открытой печати и других средствах массовой информации;
  + передача носителя информации лицу, не имеющему права доступа к ней;
  + утрата носителя с информацией.
* неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации:
  + несанкционированное изменение информации;
  + несанкционированное копирование информации;
* несанкционированный доступ к защищаемой информации:
  + несанкционированное подключение технических средств к средствам и системам ГИС «Бухгалтерия и кадры»;
  + использование закладочных устройств;
  + использование злоумышленником легальных учетных записей пользователей для доступа к информационным ресурсам ГИС «Бухгалтерия и кадры»;
  + использование злоумышленником уязвимостей программного обеспечения ГИС;
  + использование злоумышленником программных закладок;
  + заражение ГИС злоумышленником программными вирусами;
  + хищение носителей информации;
  + нарушение функционирования технических средств обработки информации;
  + блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку;
* дефекты, сбои, отказы, аварии технических средств и систем ГИС;
* дефекты, сбои, отказы программного обеспечения ГИС;
* сбои, отказы и аварии систем обеспечения ГИС;
* природные явления, стихийные бедствия:
  + термические, климатические факторы (аномально низкие или аномально высокие температуры воздуха, пожары, наводнения, снегопады и т. д.);
  + механические факторы (повреждения зданий, землетрясения и т. д.);
  + электромагнитные факторы (отключение электропитания, скачки напряжения, удары молний и т. д.).
  1. В случае возникновения нештатной ситуации, порядок действий при которой не регламентирован настоящей Политикой, Администратором, Ответственным и ГРИИБ вырабатывается конкретный план действий с учетом текущей ситуации.
  2. Порядок оповещения должностных лиц и сроки выполнения мероприятий при нештатных ситуациях определены в Приложении № 11 настоящей Политики.
  3. С целью усовершенствования координации действий должностных лиц по реагированию на нештатные ситуации должны проводиться регулярные тренировки по различным видам нештатных ситуаций. В случае выявления по результатам тренировок изъянов в положениях настоящей Политики, касающихся реагирования на нештатные ситуации, в нее могут вноситься изменения.
  4. Инциденты безопасности информации также являются нештатной ситуацией. При выявлении нештатных ситуаций, повлекших нарушение целостности, доступности или конфиденциальности защищаемой информации по вине внутреннего или внешнего нарушителя, созывается ГРИИБ, которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.
  5. В случае сбоев, отказов и аварий систем электроснабжения, вентиляции, других обеспечивающих инженерных систем предпринимаются следующие действия:
* корректное отключение технических средств ГИС до истощения ресурса источников бесперебойного питания, перегрева технических средств и до наступления других негативных последствий;
* предпринимаются меры по устранению причин, вызвавших сбои, отказы и аварии средств и систем ГИС а также меры по замене/ремонту вышедших из строя средств и систем;
* в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, баз данных, средств защиты информации, Администратор восстанавливает их из резервных копий.
  1. В случае нештатных ситуаций, связанных со стихийными бедствиями и деструктивными природными явлениями выполняются следующие действия:
* Пользователи корректно отключают и обесточивают свои рабочие места;
* системные администраторы корректно отключают и обесточивают серверы и сетевое оборудование;
* Администратор предпринимает меры к эвакуации носителей информации и носителей резервных копий;
* в случае нарушения корректной работы технических средств в ГИС в результате стихийных бедствий или природных явлений принимаются меры по ремонту/замене вышедшего из строя оборудования;
* в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, баз данных, средств защиты информации в результате стихийных бедствий или природных явлений, Администратор восстанавливает их из резервных копий;
* **в случае стихийных действий/природных явлений, опасных для жизни человека в первую очередь организуется эвакуация сотрудников и только по возможности организуется эвакуация технических средств, носителей информации и носителей с резервными копиями.**

##### {К2+} ПРАВИЛА ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОЧТЫ И ЗАЩИТЫ ОТ СПАМА

* 1. {Описать}

##### {К2+} ПРАВИЛА И ПРОЦЕДУРЫ КОНТРОЛЯ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ МОБИЛЬНОГО КОДА

* 1. {Описать}