Программный комплекс «Модель прогноза состояния информационной безопасности» (ПК МПСИБ)

Описание программы

Аннотация

Настоящий документ содержит описание программного комплекса «Модель прогноза состояния информационной безопасности» (ПК МПСИБ).

Документ предназначен для сотрудников подразделений ИБ/ ИТ и ИБ и специалистов подразделений, выполняющих контрольную функцию.

Используемые в документе термины и определения и сокращения описаны в соответствующих разделах.

Оглавление

1. Общие сведения

ПК МПСИБ является программным продуктом по прогнозированию развития ситуации в области ИБ.

Применение ПК МПСИБ позволяет снизить нагрузку на специалистов ИБ/ИТ и ИБ, прогнозировать динамику киберугроз, планировать ресурсы на предотвращение инцидентов ИБ, вести реестр информационных активов и управлять рисками ИБ, а также получать агрегированные данные для возможности контроля выполняемых процессов по ИБ.

ПК МПСИБ функционирует в составе информационных систем (ИС), построенных на основе программных продуктов «Планета».

ПК МПСИБ обеспечивает соблюдение требований следующих нормативно-правовых документов:

- Федерального закона от 27.07.2006 №149 «Об информации, информационных технологиях и о защите информации»;
- Федерального закона от 26.07.2017 №187 «О безопасности критической информационной инфраструктуры Российской Федерации»;
- Приказа Федеральной службы по техническому и экспортному контролю от 22 декабря 2017 г. №236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий».

Разработка и тестирование ПК МПСИБ выполнены в соответствии с методологией DevSecOps и в соответствии с нормами и правилами, описанными в сериях государственных стандартов ГОСТ Р 56939, ГОСТ Р ИСО/МЭК 15408, ГОСТ 2.102, ГОСТ 2.103, ГОСТ Р 51583, ГОСТ Р 51624 и в Приказах ФСТЭК №21, №76, №239.

1.1. Обозначение и наименование программы

Полное наименование: Программный комплекс «Модель прогноза состояния информационной безопасности».

Условное наименование: ПК МПСИБ.

1.2. Программное обеспечение, необходимое для функционирования ПК МПСИБ

Функциональность ПК МПСИБ реализуется в рамках ИС, использующей набор программного обеспечения (ПО), состав которого описан далее.

Операционные системы

ПК МПСИБ работает под управлением следующих операционных систем (ОС):

- Альт Сервер;
- РЕД ОС;
- Astra Linux Special Edition.

Программные продукты «Планета»

Для реализации, заложенной в ПК МПСИБ функциональности необходимо использование следующих программных продуктов «Планета»:

- «Планета. Доступ» — реализует функциональность управления авторизации, аутентификации и управления ролевой моделью;
- «Планета. Аналитика» — реализует функциональность конфигурирования, формирования и распространения отчетности и информационных панелей;
- «Планета. Сервер» — реализует функциональность конфигурирования и последующего выполнения процессов внесения изменений в основные данные;
- «Планета. Интеграция» — реализует функциональность поддержки процессов загрузки, консолидации и обработки больших объёмов данных в наборы данных для последующего анализа.

Стороннее ПО (серверы и привязка к ПО)

Для установки, развёртывания и применения ПК МПСИБ необходимо использовать программное обеспечение сторонних производителей. Состав стороннего ПО и реализуемая им функциональность зависят от конкретного проекта.

Пример набора стороннего ПО, обеспечивающего работу ПК МПСИБ в составе ИС на основе «Планета. НСИ»:

- средство контейнеризации и оркестрации — Kubernetes (Deckhouse);
- приложение балансировки нагрузки — Kubernetes;
- файловый сервер — распределенная файловая система NFS;
- сервер облачного хранилища — MinIO;
- система управления базами данных — Postgres;
- платформа управления репозиториями — Nexus.

Сведения об установке и настройке стороннего ПО содержатся в документе Руководство по установке и настройке ПК МПСИБ.

1.3. Языки программирования, на которых написана программа

Разработка прикладного программного обеспечения выполнена с использованием языка программирования высокого уровня Java.

Программирование визуальной части ПК реализовано с использованием технологий HTML, CSS и JavaScript.

Для извлечения данных из моделей в процессе функционирования ПК используется язык Python.

1.4. Типовая архитектура решения

ПК МПСИБ имеет трёхзвенную архитектуру, представленную на рисунке 1:

- клиентская часть — web-приложение;
- серверная часть — набор сервисов, реализующих бизнес-логику;
- хранилище данных — PostgreSQL, «Планета. Сервер».

Для реализации функциональности решения используются стандартные инструменты в рамках продуктов платформы «Планета»:

- «Планета. Доступ»;
- «Планета. Аналитика»;
- «Планета. Сервер»;
- «Планета. Интеграция».

При наличии соответствующих требований в рамках конкретного решения возможно развертывание дополнительных компонентов, отмеченных на рисунке 1 пунктирной линией. Например, для организации сбора и анализа метрик возможна установка инструментов Prometheus, Grafana.

Также в состав решения ПК МПСИБ интегрируются дополнительные компоненты, которые представляют из себя расширения (плагины) к продуктам платформы:

- risk-matrix;
- forecast-migration-starter.

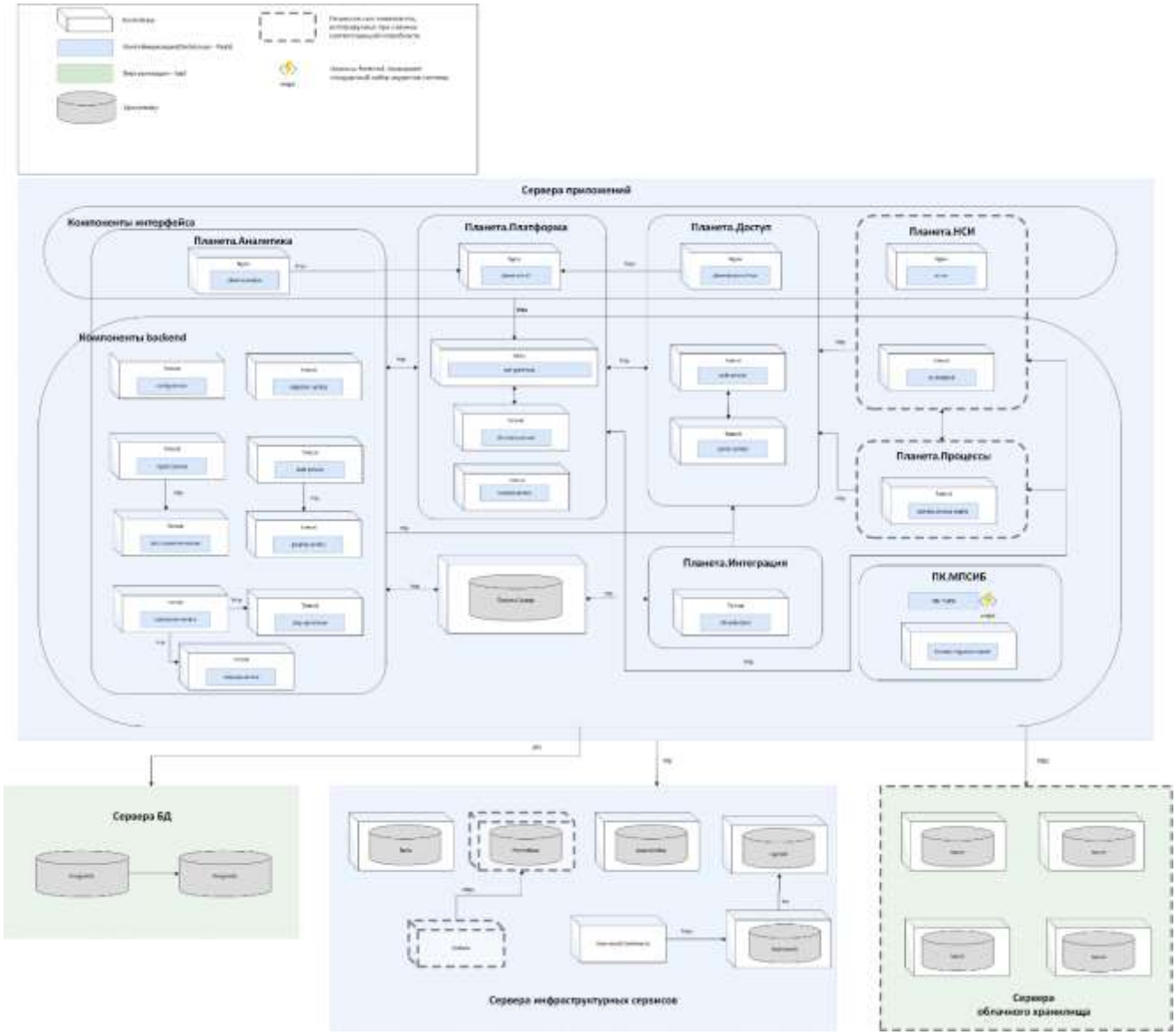

Рисунок 1.

Типовое развёртывание ПК МПСИБ выполняется при помощи ПО Kubernetes или Docker Compose. При этом часть компонентов рекомендуется устанавливать вне системы контейнеризации на уровне виртуализации, в соответствии с конкретными проектными требованиями, например, организация отказоустойчивого кластера, балансировка запросов между репликами БД.

При отсутствии специфичных требований данные компоненты разворачиваются стандартными инструментами на уровне контейнеризации.

2. Функциональное назначение

2.1. Классы решаемых задач

Применение ПК МПСИБ позволяет решать следующие задачи:

- ручной и полуавтоматический ввод данных пользователем;
- накопление и хранение данных;
- систематизация информации по отдельным признакам;
- выборка информации по определенным критериям;
- функционирование в унифицированном информационном пространстве;
- необходимая обработка информации (добавление, редактирование, удаление);
- экспорт, импорт в файлы различных форматов;
- формирование выходных форм;
- формирование выходных графиков.

2.2. Назначение программы

ПК МПСИБ предназначен для обеспечения возможности прогнозирования тенденций и характера кибератак, отражения картины развития ИБ на период 3 года, идентификации имеющихся угроз и рисков ИБ, проведения количественной оценки рисков ИБ, фиксации мероприятий по минимизации рисков ИБ, приоритизации информационных активов компании.

В частности, ПК МПСИБ обеспечивает следующие возможности:

- снижение нагрузки на специалистов ИБ/ИТ и ИБ на подготовку аналитического отчета по состоянию ИБ;
- сокращение сроков формирования отчета по состоянию ИБ;
- снижение возможности допущения ошибок при обработке данных.

3. Описание логической структуры

3.1. Алгоритм программы

Алгоритм программы основан на математическом моделировании прогноза кибератак и инцидентов на основе фактических данных за прошлые периоды; на идентификации угроз и рисков ИБ информационных активов в соответствии с БДУ ФСТЭК.

3.2. Используемые методы

Методы прогнозирования (линейная регрессия).

Таблицы маппинга (таблица xls).

Система присвоения баллов.

Возможные обновления таблицы (состав).

3.3. Структура программы с описанием функций составных частей и связи между ними

Схема структуры ПК МПСИБ представлена на рисунке 1.

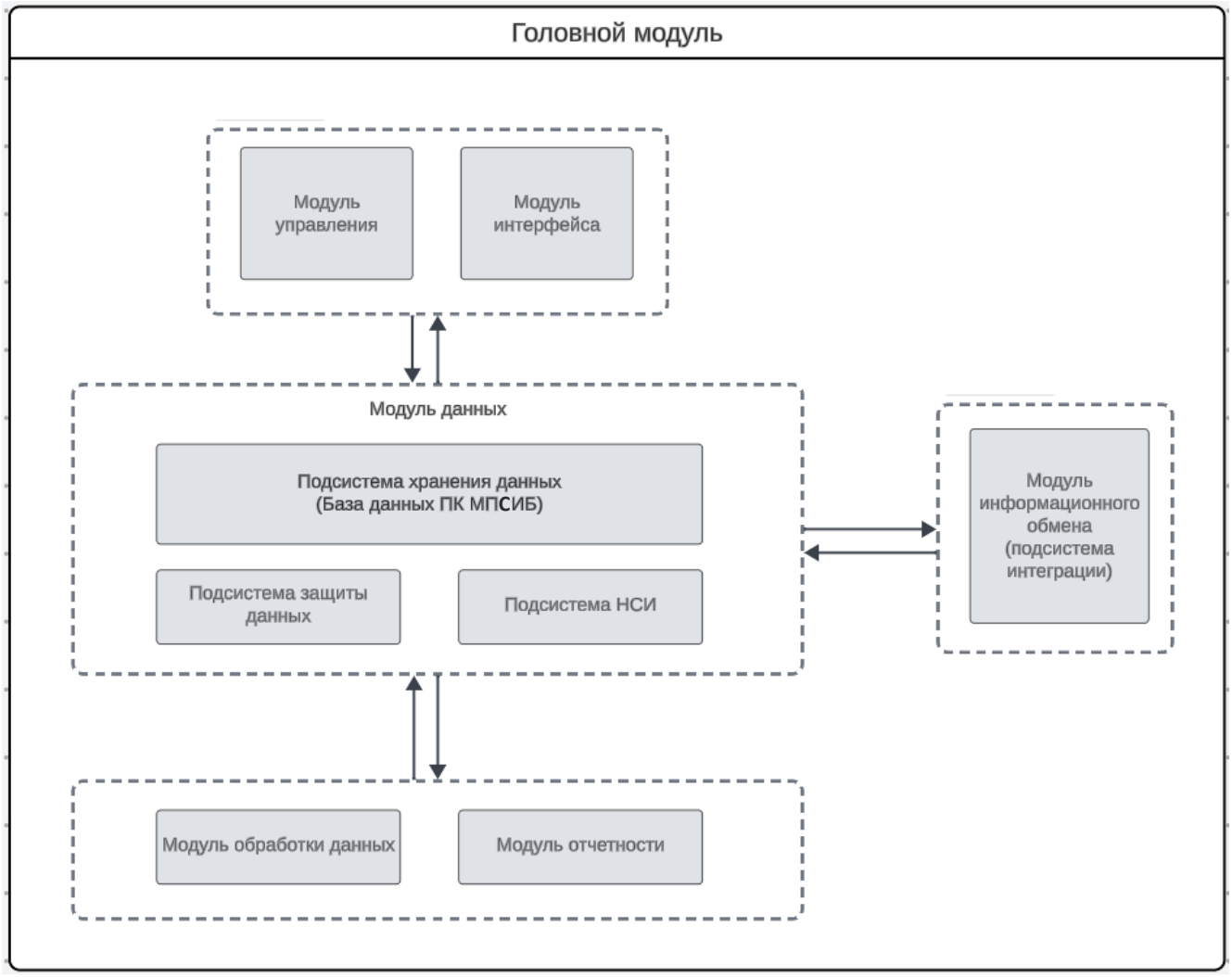

Рисунок 1

ПК МПСИБ представляет собой набор следующих программных компонентов:

- головной модуль — ядро системы, отвечает за работу системы, является основой для всех модулей системы и функционала, отвечает за связь модулей и общую работоспособность. Реализует функционирование базовых надстроек системы. В рамках головного модуля представлены подмодули Управления и Интерфейса.
    - подмодуль управления — содержит весь перечень настроек среды для определения, регулирования визуальной и функциональной составляющих, администрирования системы, системные элементы, вызывающие главное меню и вспомогательные панели управления;
    - подмодуль интерфейса — организует диалог пользователя с программным комплексом. В зависимости от действий пользователя модуль передает осведомительные сигналы основному модулю, а в зависимости от управляющих сигналов от основного модуля, выводит конкретную информацию пользователю. Осуществляет

контроль над действиями пользователя, ограничивая диапазон допустимых символов при вводе информации с клавиатуры;

- модуль обработки данных — предназначен для ввода, обработки и упорядочивания, анализа и сбора данных. Модуль построен на основе современных OLAP-технологий, позволяющих создавать многомерные аналитические отчеты произвольного вида;
- модуль информационного обмена — содержит в себе подсистему интеграции. Подсистема интеграции обеспечивает приём запросов от смежных систем, обработку полученных запросов и предоставление ответов на запросы и передачу запросов в смежные системы и обработку полученных ответов. К смежным системам относятся:
    - модуль формирования отчетности — содержит подсистемы визуального структурирования и представления данных в различных форматах;
    - модуль данных — модуль содержит подсистемы для работы с нормативно-справочной информацией, хранения данных, а также их защиты. Модуль представляет собой группу, состоящую из трёх подсистем:
        - подсистемы управления нормативно-справочной информацией, обеспечивающей ведение справочников и реестров;
        - подсистемы защиты информации — программно-технического комплекса, предназначенного для защиты технических средств, программного обеспечения и данных от несанкционированного доступа к данным ПК МПСИБ;
        - подсистемы хранения данных (БД ПК МПСИБ), осуществляющей хранение оперативных данных системы, данных для формирования аналитических отчетов и документов системы, сформированных в процессе работы отчетов.

3.4. Связи программы с другими программами

Основные требования, предъявляемые к совместимости обмена данными между компонентами ПК МПСИБ и внешними системами:

- единые форматы импорта/экспорта данных;
- использование стандартизованных протоколов и интерфейсов обмена данными.

Смежными системами для ПК МПСИБ являются система сбора данных при осуществлении обследования и аудита ИБ, а также при моделировании угроз ИБ.

4. Используемые технические средства

В состав ПК МПСИБ входят следующие технические средства:

- серверы БД;
- веб-интерфейс;
- сервер системы формирования отчетности.

Для функционирования ИС необходима локальная вычислительная сеть на основе протокола TCP/IP с пропускной способностью 10/100 Мбит/с.

4.1. Типы электронных вычислительных машин и устройств, которые используются при работе программы

ПК МПСИБ использует для работы серверы и рабочие станции (персональные компьютеры).

Требования к серверам

Сервер платформы контейнеризации (master):

- количество серверов не менее 3 шт.;
- CPU — 4 ядра;
- объём памяти RAM — 8 Гб;
- объём хранения данных — 200 Гб.

Сервер инфраструктурных сервисов (worker):

- количество серверов не менее 2 шт.;
- CPU — 4 ядра (рекомендовано 16 ядер);
- объём памяти RAM — 8 Гб (рекомендовано 32 Гб);
- объём хранения данных — 200 Гб.

Файловый сервер:

- CPU — 4 ядра;
- объём памяти RAM — 16 Гб
- объём хранения данных — 5 Тб.

Сервер облачного хранилища:

- CPU — 4 ядра;
- объём памяти RAM — 16 Гб;
- объём хранения данных — 532 Гб.

Сервер БД:

- CPU — 32 ядра;
- объём памяти RAM — 96 Гб;
- объём хранения данных — 1 Тб.

Платформа управления репозиториями

- CPU — 4 ядра;
- объём памяти RAM — 8 Гб;
- объём хранения данных — 200 Гб.

Требования к рабочим станциям (персональным компьютерам)

Рабочие станции (персональные компьютеры пользователей и администраторов) должны обладать следующими техническими характеристиками:

- CPU — 2 ядра;
- объём памяти RAM — 4 Гб;
- объём хранения данных — 32 Гб;
- монитор SVGA;
- клавиатура 101/102 клавиши;
- манипулятор типа «мышь»;
- устройство чтения компакт-дисков (DVD-ROM);
- сетевой адаптер 100 Мбит/с.

Программное обеспечение рабочих станций должно работать под управлением ОС Astra Linux 1.7 Орёл (минимальная версия) и позволять использование ПО Microsoft Office 2003 (минимальная версия).

На рабочих станциях должны запускаться актуальные версии одного из следующих веб-браузеров: Mozilla FireFox, Яндекс.Браузер, Google Chrome.

5. Вызов и загрузка

5.1. Способ вызова программы с соответствующего носителя данных

ПК МПСИБ может вызываться следующими способами:

- как программный модуль, запускаемый с носителя информации.

При загрузке ПК выполняется двухфакторная аутентификация.

Загрузка рабочего стола пользователя осуществляется в соответствии с назначенной ему ролью. Для аутентифицированного пользователя на загруженном рабочем столе отображается набор вкладок отчётов и справочников.

Перед открытием выбранного отчёта выполняется загрузка данных обследования ИТ-инфраструктуры пользователя и актуализация справочников ФСТЭК.

5.2. Входные точки в программу

1. Открытая информация — актуализируемые данные об угрозах ИБ и уязвимостях ПО с портала ФСТЭК. Действие выполняется оператором (пользователем).
2. Отчетные формы, содержащие сведения о текущих ИА и статистике атак и инцидентов за 3 года.

6. Входные данные

6.1. Характер, организация и предварительная подготовка входных данных

Входными данными для ПК МПСИБ являются следующие:

- информация, извлечённая из опросных листов обследований и аудита ИБ. Экспорт данных выполняется посредством загрузки данных в формате загрузочных файлов excel «Аналитика_ИА» и «Аналитика_Инциденты» в раздел **Аналитика** ПК МПСИБ;
- набор справочников базы данных уязвимостей ФСТЭК (БДУ ФСТЭК), проверяемых на актуальность дат публикации;
- сведения об оценке критичности ИС, участвующих в бизнес-процессах.

Предварительная подготовка входных данных выполняется в соответствии с определённым шаблоном загрузки, строго регламентирующим набор данных для конкретной задачи.

Предусмотрена возможность использования «Автоматизированного помощника» (чат-бот) для сбора и подготовки аналитических данных по ИА и атакам и инцидентам.

Шаблон загрузки должен быть заполнен в строгом соответствии со справочником БДУ ФСТЭК.

6.2. Формат, описание и способ кодирования входных данных

Собранные в соответствии с шаблоном данные обрабатываются в «Планета. Аналитика», после чего передаются в ПК МПСИБ, где выполняются их оценка и применение.

7. Выходные данные

Выходными данными для ПК МПСИБ являются:

- сводный отчёт по кибератакам и инцидентам;
- реестр информационных активов;
- карточки информационных активов, разделённые по следующему принципу:
    - данные статистики и прогнозов атак и инцидентов;
    - данные оценки рисков и угроз ИБ, меры по минимизации рисков/угроз ИБ (в соответствии с требованиями ФСТЭК);
- реестр рисков ИБ с наименованием и оценкой рисков.
- матрица рисков;
- сформированные выходные формы;
- сформированные выходные графики.

Сформированные в ПК МПСИБ отчеты могут служить входными данными для смежных ИС.

7.1. Характер и организация выходных данных

Кубы in-memory OLAP «Планета. Сервер» — хранилище информации. Формат хранения данных — собственный, свой формат файлов.

Инфопанели — основной способ отображения информации пользователю.

Выгрузка из MS Excel (выполняется вне ПК).

7.2. Формат, описание и способ кодирования выходных данных

XLS, PDF и формат кубов данных.

Термины и определения

Термин	Определение
Администратор	Сотрудник организации, обладающий компетенциями и правами для управления ИС
Информационная панель	Набор элементов интерфейса ИС, обеспечивающий визуализацию данных о состоянии компонентов
Информационная система (ИС)	Совокупность программных продуктов, использование которых позволяет выполнять определённые задачи автоматизации бизнес-процессов, имеющих критическую значимость и влияющих на финансовую деятельность заказчика
Информационный актив (ИА)	Информация, несущая ценность для организации в интересах достижения целей деятельности и находится в ее распоряжении, имеющая материальную и нематериальную форму, например, информация, программное обеспечение, компьютер, услуги, люди и их квалификация, навыки и опыт, репутация и имидж
Программные продукты «Планета»	Набор разработанных ГК ИБС программных продуктов, обеспечивающих решение различных корпоративных задач в области обработки данных и управления данными и процессами компании
Программный компонент	Часть программного обеспечения ИС, выполняющая определённые задачи
Справочник	Сущность ИС, содержащая определённые данные и позволяющая их обработку

Сокращения

Сокращение	Значение
БД	База данных
ИС	Информационная система
НСИ	Нормативно-справочная информация
ПО	Программное обеспечение
СУБД	Система управления базами данных
HTTP	HyperText Transfer Protocol (протокол передачи гипертекста) — сетевой протокол прикладного уровня
TCP	Transmission Control Protocol (протокол управления передачей) — сетевая модель, описывающая процесс передачи цифровых данных