УТВЕРЖДАЮ

Президент-председатель правления ПАО «ЗенитБанк»

_____/_____ /

«___» _____ 20__г.

МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ЕЕ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ БАНКА “ПАО ЗЕНИТБАНК”

Публичное акционерное общество «ЗенитБанк»

Москва 2023

Содержание

Перечень принятых сокращений

ИСПДн — информационная система персональных данных

КЗ — контролируемая зона

НДВ — недекларированные возможности

НСД — несанкционированный доступ

ОБПДн — обеспечение безопасности персональных данных

ПДн — персональные данные

ПО — программное обеспечение

СВТ — средство вычислительной техники

СЗИ — средство защиты информации

ТКУ И — технический канал утечки информации

УБПДн — угрозы безопасности персональных данных

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Назначение Модели угроз

Разработка Модели угроз выполняется для определения актуальных угроз безопасности защищаемой информации, обрабатываемой в АИСПД ПАО ЗенитБанк.

Результаты определения актуальных угроз безопасности защищаемой информации предназначены для формирования обоснованных требований к составу и содержанию мер по обеспечению информационной безопасности АИСПД ПАО ЗенитБанк.

1.2. Нормативно-правовые акты, методические документы, используемые для оценки угроз безопасности информации и разработки Модели угроз

Нормативной основой настоящей модели являются законодательство Российской Федерации и нормы права в части обеспечения информационной безопасности, требования нормативных актов Центрального Банка Российской Федерации, Федерального органа исполнительной власти, уполномоченного в области безопасности, Федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, и основывается, в том числе

− Федеральный закон от 27.06.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

− Федеральный закон от 27.06.2006 г. № 152-ФЗ «О персональных данных»;

− Федеральный закон от 27.06.2011 г. № 161-ФЗ «О национальной платежной системе»;

− Федеральный закон от 02.12.1990 г. № 395-1 «О банках и банковской деятельности»;

− Федеральный закон от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне»; − Положение Банка России от 09.06.2012 г. № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»;

− Положение Банка России от 09.01.2019 г. № 672-П «О требованиях к защите информации в платежной системе»;

− Положение Банка России от 17.04.2019 г. № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств»;

− Положение Банка России от 08.04.2020 г. № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе»;

− Указание Банка России от 09.06.2012 г. №2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств»;

− Стандарты Банка России (СТО БР ИББС); − Рекомендации в области стандартизации Банка России (РС БР ИББС);

− Национальный стандарт Российской Федерации ГОСТ Р 57580.1-2017 «Безопасности финансовых (банковских) операций. Защита информации финансовых 9 организаций. Базовый состав организационных и технических мер»

1.3. Область применения настоящей Модели угроз

Информационная система персональных данных «ПАО Банка ЗенитБанк»» (далее — ИСДн ЗенитБанка) предназначена для формирования, обработки, хранения и предоставления данных о работе ЗенитБанка в рамках отношений. указанных в Федеральном законе от 09.02.2009 № 8-ФЗ «Об

обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления».

Решение о создании ИСПДн ЗенитБанка принято на основании приказа от 10.08.2020 N2 87-0 «О защите информании».

В соответствии с актом классификации ИСПДн ЗенитБанка от 10.08.2020 №88-о утверждённым директором и по результатам анализа исходных данных ИСПДн ЗенитБанка имеет 4 уровень защищенности персональных данных (УЗ 4).

В ИСПДн ЗенитБанка могут обрабатываться следующие персональные данные: фамилия, имя, отчество;

место, год, дата рождения; адрес проживания;

адрес электронной почты;

сведения об образовании;

сведения о трудовой деятельности;

сведения о трудовом стаже;

телефонный номер;

семейное положение;

данные о наградах, медалях, поощрениях, почетных званиях;

В соответствии со статьей 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных». оператор ИСПДн ЗенитБанка при обработке персональных данных (далее - ПДн) обязан принимать правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного достмла к ним. уничтожения, изменения, блокирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн. Мероприятия по обеспечению безопасности ПДн при их обработке в ИСПДн ЗенитБанка включают в себя определение угроз безопасности ПДн при их обработке и формирование Модели угроз.

Модель угроз содержит данные по угрозам, связанным с несанкционированным, в том числе случайным. доступом в ИСПДн

ЗенитБанка с целью изменения, неправомерного распространения информации или деструктивных воздействий на элементы ИСПДн и обрабатываемых в них информации с использованием программных и программно-аппаратных средств с целью уничтожения или блокирования защищаемой информации.

В Модели угроз представлена оценка исходного уровня защищенности защищаемой информации, а также анализ угроз безопасности информации.

Анализ угроз безопасности информации включает: описание угроз; оценку вероятности возникновения угроз; оценку реализуемости угроз; оценку опасности угроз; определение актуальности угроз.

К информационным ресурсам ИСПДн ЗенитБанка осуществляется удаленный доступ сотрудников других организаций по незащищенному каналу связи.

1.4. Наименование обладателя информации, заказчика, оператора систем и сетей: ПАО “ЗенитБанк”

1.5. Подразделения, должностные лица, ответственные за обеспечение защиты информации (безопасности) систем и сетей

Подразделениями, отвечающими за обеспечение защиты информации

Подсистемы, выступают:

- Управление режима безопасности информации Заказчика.

1.6. Наименование организации, привлекаемой для разработки модели угроз безопасности информации (при наличии)

Отсутствует, разработка произведена собственными силами.

2 ОПИСАНИЕ СИСТЕМ И СЕТЕЙ И ИХ ХАРАКТЕРИСТИКА КАК ОБЪЕКТОВ ЗАЩИТЫ

2.1. Наименование систем и сетей, для которых разработана модель угроз безопасности информации:

– объект 1 – информационная система персональных данных «ПАО ЗенитБанк»;

– объект 2 – ЛВС, в рамках которой работники обеспечивают обмен информацией;

– объект 3 – сервер, на котором хранятся БД ИСПДн, «ПАО Банк ЗенитБанк».

2.2. Класс защищенности, категория значимости систем и сетей, уровень защищенности персональных данных

Защита информации, включая персональные данные, в банковской сфере, регулируется законодательством и стандартами, которые устанавливают требования к классу защищенности, категории значимости систем и сетей, а также уровню защиты персональных данных. В контексте ИСПДн (Информационные системы, обрабатывающие персональные данные), типично применяются следующие параметры:

1) Класс защищенности: Класс защищенности определяется в соответствии с уровнем конфиденциальности информации, обрабатываемой в ИСПДн Банка. В банковской сфере часто применяются следующие классы:

Класс 1: Открытая информация (публично доступная).

Класс 2: Информация с ограниченным доступом (например, информация о клиентах без банковских секретов).

Класс 3: Конфиденциальная информация (содержит банковские секреты и другую чувствительную информацию).

2) Категория значимости систем и сетей: Категория значимости определяет важность ИСПДн для банка и клиентов. Категории значимости могут быть разные, но обычно выделяются следующие:

Категория 1: Критически важные системы и сети (например, банковские транзакции и онлайн-банкинг).

Категория 2: Значимые системы и сети, но не критически важные (например, внутренние порталы и системы управления ресурсами).

Категория 3: Незначимые системы и сети (например, внутренние тестовые системы).

Уровень защиты персональных данных: Это определяется в соответствии с требованиями законодательства о защите персональных данных ФЗ "О персональных данных" .

Уровень защищенности ИСПДн Банка ЗенитБанка – четвертый.

2.3. Нормативно правовые акты Российской Федерации, в соответствии с которыми создаются и (или) функционируют системы и сети

Настоящая Политика разработана в соответствии с положениями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее в тексте – Закон № 152-ФЗ), а также иными подзаконными нормативно-правовыми актами в сфере персональных данных.

2.4. Назначение, задачи (функции) систем и сетей, состав обрабатываемой информации и ее правовой режим; основные процессы обладателя информации, для обеспечения которых создаются (функционируют) системы и сети

ИСПДн ЗенитБанка предназначена для обеспечения безопасной и эффективной обработки, хранения и защиты персональных данных клиентов и сотрудников. Основной целью является соблюдение требований законодательства о защите персональных данных, предоставление услуг клиентам и управление внутренними данными о сотрудниках.

В ИСПДн ЗенитБанка могут обрабатываться следующие персональные данные:

Информацию о клиентах: имена, адреса, номера телефонов, паспортные данные, финансовые данные и иная информация, необходимая для предоставления банковских услуг.

Информацию о сотрудниках банка: имена, данные о занятости, информация о заработной плате, налоговая и социальная информация и др.

Основные задачи(функции) ИСПДн Банка ЗенитБанк:

Сбор и регистрация персональных данных клиентов при оказании услуг, например, открытие счетов или выдача кредитов.

Хранение и обработка персональных данных, включая их защиту от несанкционированного доступа и утечек.

Обеспечение прав клиентов на доступ и управление своими данными.

Обеспечение соответствия законодательству о защите персональных данных, включая уведомления о нарушениях безопасности данных.

Обеспечение безопасности информации о сотрудниках банка.

2.5. Основные процессы обладателя информации, для обеспечения которых создаются (функционируют) системы и сети:

Банк ЗенитБанк создает и поддерживает системы и сети для информационных систем персональных данных (ИСПДн) с целью обеспечения ряда ключевых процессов, которые гарантируют безопасное и эффективное управление персональными данными клиентов и сотрудников. Основные процессы обладателя информации, для которых создаются и функционируют системы и сети ИСПДн банка, включают в себя:

- Сбор и регистрация данных;
- Хранение и обработка данных;
- Управление доступом и авторизация;
- Обеспечение прав клиентов на доступ и контроль данных:
- Мониторинг и обнаружение инцидентов безопасности

- Управление рисками в области безопасности данных: риски и защитить данные;

- Реагирование на инциденты безопасности и уведомление о нарушениях.

2.6. Описание групп внешних и внутренних пользователей систем и сетей, уровней их полномочий и типов доступа (в состав групп пользователей включается все пользователи, для которых требуется авторизация при доступе к информационным ресурсам, и пользователи, для которых не требуется авторизация

Таблица 1 – Описание групп пользователей

Типовая роль	Уровень доступа к ИСПДн	Разрешенные действия в ИСПДн
Администратор ИСПДн (администратор системы-)	Обладает полной правами права на управление и настройку системы ИСПДн, полные права на настройку и конфигурацию системы, полный мониторинг и аудит системы, полное управление резервными копия и восстановлением данные	Полный доступ для администрирования, настройки безопасности и мониторинга системы. То есть удаление УЗ, добавление УЗ
Сотрудники Банка	В зависимости от должности в Банке. Сотрудники Банка обладают полной информацией о собственных данных, Сотрудники Банка(менеджеры по обслуживанию клиентов) частичное обладают информациях о клиентках банка(история транзакций, договора). Сотрудники Банка(Бухгалтерия и финансовые аналитики) имеют доступ к финансовым данным. Сотрудники Банка(отдел кадров и управления персоналом) имеют доступ к ПДн сотрудника Банка.	Ограниченный доступ к данным клиентов и сотрудников в соответствии с их должностными обязанностями.
Ответственные за безопасность данных	Обладают полномочиями для настройки и мониторинга безопасности данных.	Доступ к средствам защиты, мониторингу безопасности и расследованию инцидентов.
Клиенты Банка	Обладают доступом к собственным данным, обработка личной информации, выполнение банковских операций.	Ограниченные действия со своими собственных данных, доступ к услугам банка.
Регуляторы и Аудиторы	Обладают полными правами для аудита и проверки соответствия законодательству.	Проведение аудитов и проверок, включая доступ к данным клиентов и сотрудников при выполнении своих функций.
Партнеры и поставщики услуг	Обладают ограниченным доступ к данным, необходимым для выполнения соглашений и обеспечения услуг.	Ограниченный доступ в рамках согласованных соглашений и необходимых операций.

2.7 Описание функционирования систем и сетей на базе информативно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры:

Не реализовано.

2.8 Описание модели предоставления вычислительных услуг, распределения ответственности за защиту информации между обладателями информации, оператором и поставщиком вычислительных услуг

Не реализовано.

2.9 Описание условий использования информационно-телекоммуникационной инфраструктуры обработки данных или облачной инфраструктуры поставщика услуг (при наличии)

Не реализовано.

3. Возможные объекты воздействия угроз безопасности информации. Возможные негативные последствия реализации угроз безопасности информации.

Таблица 2 – Описание групп пользователей

Негативные последствия	Объекты воздействия	Виды воздействия
Потеря (хищение) денежных средств	Банк-клиент	Несанкционированная подмена данных, содержащихся в реквизитах платежного поручения
	АРМ финансового Директора ЗенитБанк	Несанкционированная модификация информации в платежных распоряжениях и отправка недостоверных распоряжений от имени финансового директора
	Электронный почтовый ящик финансового директора ЗенитБанк	Модификация информации в платежных распоряжениях и отправка недостоверных распоряжений от имени финансового директора
	АРМ главного бухгалтера	Подмена данных, содержащих реквизиты платежных поручений и другой платежной информации на АРМ главного бухгалтера
Невозможность заключения договоров, соглашений	АРМ руководителя Службы в Банке ЗенитБанк	Модификация информации и отправка электронных писем с недостоверной информацией от имени руководителя организации
	Электронный почтовый ящик руководителя организации	Модификация информации и отправка электронных писем с недостоверной информацией от имени руководителя организации
Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса	АРМ руководителя Администрирования в ЗениБанк	Модификация информации и отправка электронных писем с недостоверной информацией от имени руководителя организации
	АРМ главного инженера/администратора ЗенитБанк	Несанкционированная отправка команд, приводящая к несрабатыванию средств аварийной защиты и (или) к изменению логики ПЛК
Причинение имущественного ущерба	АРМ главного инженера	Несанкционированная отправка команд, приводящая к несрабатыванию средств аварийной защиты и (или) к изменению логики ПЛК
	АРМ оператора	Несанкционированная отправка команд, приводящая к несрабатыванию средств аварийной защиты и (или) к изменению логики ПЛК
	Коммутационный контроллер для управления аварийными задвижками в нефтепроводе	Несанкционированная модификация (изменение) логики работы или уставок коммутационного контроллера, которая приводит к открытию (или не закрытию) аварийной задвижки при нарушении герметичности нефтепровода
Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.)	АРМ руководителя организации	Модификация информации и отправка электронных писем с недостоверной информацией от имени руководителя организации

4. ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. СПОСОБЫ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОТИ ИНФОРМАЦИИ.

Таблица 3 – Возможные цели реализации угроз безопасности информации нарушителями

№ вида	Виды нарушителя	Категории нарушителя	Возможные цели реализации угроз ИБ
1	Преступные группы (криминальные структуры)	Внешний	Получение финансовой или иной материальной выгоды. Дестабилизация деятельности Банка ЗенитБанк
2	Конкурирующие организации	Внешний	Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды
3	Разработчики программных, программно-аппаратных средств	Внутренний	Внедрение дополнительных функциональных возможностей в программные или программно-аппаратные средства на этапе разработки. Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия
5	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ
6	Системные администраторы и администраторы безопасности	Внутренний	Получение финансовой и материальной выгоды. Месть за ранее совершенные действия. Любопытство или желание самореализации. Непреднамеренные, неосторожные или неквалифицированные действия

Таблица 4 – Оценка целей реализации нарушителями угроз безопасности информации в зависимости от возможных негативных последствий и видов ущерба от их реализации

Виды нарушителей	**Возможные цели реализации угроз безопасности информации**	**Соответствие целей видам риска (ущерба) и возможным негативным последствиям**
	Риски юридическому лицу,работающему в банке Руководство Банка, связанные с хозяйственной деятельностью	
Разработчики программных, программно-аппаратных средств	+ (передача информации о предприятии третьим лицам)	У2 (утечка коммерческой тайны)
Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	+ (дестабилизация деятельности Банка)	У2 (потеря денежных средств; нарушение штатного режима функционирования объекта)
Системные администраторы и администраторы безопасности	+ (получение финансовой или иной материальной выгоды при вступлении в сговор с преступной группой)	У2 (хищение денежных средств Банка)
Преступные группы (криминальные структуры)	+ (дестабилизация деятельности Банка)	У2 (утечка коммерческой тайны; причинение имущественного ущерба;)
Конкурирующие организации	+ (дестабилизация деятельности Банка)	У2 (невозможность заключения договоров;)

5. СПОСОБЫ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ.

Таблица 5 – Определение актуальных способов реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
1	Преступные группы (два лица и более, действующие по единому плану)	Внешний	Доступ к базам данных	Веб-интерфейс удаленного администрирования базы данных информационной системы Пользовательский веб-интерфейс доступа к базе данных информационной системы	Использование уязвимостей конфигурации системы управления базами данных
			Удаленное рабочее место пользователя	Доступ через локальную вычислительную сеть организации	Внедрение вредоносного ПО; использование уязвимостей системы
2	Конкурирующие организации	Внешний	Доступ к базам данных	Веб-интерфейс удаленного администрирования базы данных информационной системы Пользовательский веб-интерфейс доступа к базе данных информационной системы	Использование уязвимостей конфигурации системы управления базами данных
			Удаленное рабочее место пользователя	Доступ через локальную вычислительную сеть организации	Внедрение вредоносного ПО; использование уязвимостей системы
3	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Доступ к базам данных	Веб-интерфейс удаленного администрирования базы данных информационной системы Пользовательский веб-интерфейс доступа к базе данных информационной системы	Использование уязвимостей конфигурации системы управления базами данных
			АРМ оператора	Съемные машинные носители информации, содержащие аутентификационную информацию	Извлечение аутентификационной информации из постоянной памяти носителя
			Коммутационный контроллер для управления аварийным	Удаленный канал управления коммутационным контроллером	Использование уязвимостей кода; кража аутентификационной информации из

			задвижками в нефтепроводе:	Съемные машинные носители информации, содержащие аутентификационную информацию	постоянной памяти носителя
4	Системные администраторы и администраторы безопасности	Внутренний	Доступ к базам данных	Веб-интерфейс удаленного администрирования базы данных информационной системы Пользовательский веб-интерфейс доступа к базе данных информационной системы	Использование уязвимостей конфигурации системы управления базами данных
			Удаленное рабочее место пользователя	Доступ через локальную вычислительную сеть организации Съемные машинные носители информации, подключаемые к АРМ пользователя	Использование уязвимостей конфигурирования системы; установка вредоносного ПО
			Линия связи между сервером основного центра обработки данных и сервером резервного центра обработки данных:	Канал передачи данных между сервером основного центра обработки данных и сервером резервного центра обработки данных	Установка закладок
5	Разработчики программных, программно-аппаратных средств	Внутренний	Доступ к базам данных	Веб-интерфейс удаленного администрирования базы данных информационной системы Пользовательский веб-интерфейс доступа к базе данных информационной системы	Использование уязвимостей конфигурации системы управления базами данных
			Удаленное рабочее место пользователя	Доступ через локальную вычислительную сеть организации Съемные машинные носители информации, подключаемые к АРМ пользователя	Использование уязвимостей конфигурирования системы; установка вредоносного ПО

6. АКТУАЛЬНЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. Определение исходного уровня защищенности ИСПДн

Для выявления из всего перечня угроз безопасности персональных данных актуальных для информационной системы персональных данных оцениваются два показателя:

- уровень исходной защищенности информационной системы персональных данных;

- частота (вероятность) реализации рассматриваемой угрозы.

Под уровнем исходной защищенности информационной системы персональных данных (ИСПДн) понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн, а именно:

- территориальное размещение;

- наличие соединению сетями общего пользования;

- встроенные (легальные) операции с записями баз персональных данных;

- разграничение доступа к персональным данным;

- наличие соединений с другими базами персональных данных иных ИСПДн;

- уровень обобщения (обезличивания) персональных данных;

- объем персональных данных, который предоставляется сторонним пользователям ИСПДн без предварительной обработки.

ФСТЭК России выделило 3 (три) уровня исходной защищенности ИСПДн (Y_1):

- высокий;

- средний;

- низкий.

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик информационной системы персональных данных. Перечень данных характеристик и показатели защищенности информационной системы персональных данных, зависящие от них, показаны в таблице 6.

Показатели, относящиеся к ИСПДн Банка ЗенитБанк выделены зеленым цветом .

Таблица 6 – Показатели исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	**Уровень защищенности**		
	Высокий	**Средний**	**Низкий**
1. По территориальному размещению:	+		
распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;	–	–	–
городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка);	–	–	–
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;	+	–	–
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;	+	–	–
локальная ИСПДн, развернутая в пределах одного здания	+	–	–
2. По наличию соединения с сетями общего пользования:	+		
ИСПДн, имеющая многоточечный выход в сеть общего пользования;	–	–	–
ИСПДн, имеющая одноточечный выход в сеть общего пользования;	–	–	–
ИСПДн, физически отделенная от сети общего пользования	+	–	–
3. По встроенным (легальным) операциям с записями баз персональных данных:	+		
чтение, поиск;	+	–	–
запись, удаление, сортировка;	+	–	–
модификация, передача	+	–	–
4.По разграничению доступа к персональным данным:	+		

ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;	+	–	–
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;	–	–	–
ИСПДн с открытым доступом	–	–	–
5. По наличию соединений с другими базами ПДн иных ИСПДн:		+	
интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн);	–	–	–
ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	–	–	–
6. По уровню обобщения (обезличивания) ПДн:	+		
ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);	+	–	–
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	–	–	–
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	–	–	–
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:	+		
ИСПДн, предоставляющая всю базу данных с ПДн;	–	–	–
ИСПДн, предоставляющая часть ПДн;	–	–	–
ИСПДн, не предоставляющая никакой информации.	+	–	–

6.2. Правила определения исходного уровня защищенности ИСПДн

Исходная уровень защищенности ИСПДн определяется следующим образом.

1. ИСПДн имеет **высокий** уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню «высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные –

среднему уровню защищенности (положительные решения по второму столбцу).

Таблица 7 – Условия определения высокого уровня исходной защищенности

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
ИТОГО	$\sum \geq 70\%$	$\sum \leq 30\%$	0%

ИСПДн имеет средний уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний» (берется отношение суммы положительные решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные – низкому уровню защищенности.

Таблица 8 – Условия определения среднего уровня исходной защищенности

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
ИТОГО	$\sum < 70\%$	$\sum \geq 70\%$	$\sum \leq 30\%$

ИСПДн имеет низкую степень исходной защищенности, если не выполняются условия по пунктам 1 и 2.

Таблица 9 – Условия определения низкого уровня исходной защищенности

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
ИТОГО	$\sum < 70\%$	$\sum < 70\%$	$\sum > 0\%$

При составлении перечня актуальных угроз безопасности персональных данных каждой степени исходного уровня защищенности ИСПДн ставится в соответствие числовой коэффициент Y_1, а именно:

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

10 – для низкой степени исходной защищенности

По результатам, **ИСПДн Банка ЗенитБанк** соответствует **высокому** уровню защищенности.

6.3. Правила отнесения угрозы безопасности ПДн к актуальной

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя:

маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);

низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);

средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;

высокая вероятность - объективные предпосылки для реализации угрозы существуют, и меры по обеспечению безопасности ПДн не приняты.

При составлении перечня актуальных угроз безопасности ПДн каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент, а именно:

0 – для маловероятной угрозы;

2 – для низкой вероятности угрозы;

5 – для средней вероятности угрозы;

10 – для высокой вероятности угрозы.

С учетом изложенного коэффициент реализуемости угрозы Y будет определяться соотношением.

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

если, то возможность реализации угрозы признается низкой;

если, то возможность реализации угрозы признается средней;

если, то возможность реализации угрозы признается высокой;

если, то возможность реализации угрозы признается очень высокой.

Далее оценивается опасность каждой угрозы. При оценке опасности на основе опроса экспертов (специалистов в области защиты информации) определяется вербальный показатель опасности для рассматриваемой ИСПДн. Этот показатель имеет три значения:

низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Таблица 10 – Правила отнесения угрозы безопасности ПДн к актуальной

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальна	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная