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».

В соответствии с актом классификации ИСПДн ЗенитБанка от 15.11.23 №785-о утверждённым президентом-председателя правления 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.

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 выступают:

- Управление по обеспечению информационной безопасности
- Департамент поддержки и контроля, администрирования безопасности.

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

Отсутствует, разработка произведена собственными силами.

1.7. Особенности пересмотра Модели угроз

Модель угроз может быть пересмотрена в следующих случаях:

– По решению Оператора информации, основанному на регулярном анализе и оценке угроз безопасности защищаемой информации с учетом изменений в системах и сетях.

– В случае обнаружения новых уязвимостей и угроз безопасности информации, что требует актуализации и улучшения предоставленной модели.

– При изменении федерального законодательства, касающегося оценки угроз безопасности информации, для соответствия актуальным правовым требованиям и нормам.

Кроме того, пересмотр может произойти при появлении новых угроз в используемых источниках данных об угрозах безопасности, изменении структурно-функциональных характеристик информационных технологий и особенностей функционирования систем и сетей, а также при появлении сведений о новых возможностях потенциальных нарушителей и выявлении инцидентов информационной безопасности в системах и сетях. Такой подход обеспечивает регулярное обновление Модели угроз, чтобы эффективно справляться с постоянно меняющейся угрозовой средой.

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 Модель Угроз ИСПДн Банка ЗенитБанк 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.

В рамках процесса моделирования угроз безопасности информации, пвключены следующие этапы:

- Анализ возможных негативных последствий, которые могут возникнуть при осуществлении угроз безопасности информации.
- Выявление условий, при которых угрозы безопасности информации могут быть реализованы.
- Идентификация источников угроз безопасности информации и оценка потенциальных возможностей нарушителей.
- Определение сценариев, в рамках которых могут осуществиться угрозы безопасности информации.

В таблице 2 представлены процессы моделирование угроз безопасности информации.

Таблица 2 – Моделирования угроз безопасности информации

ВХОДНЫЕ ДАННЫЕ	ЭТАП	ПОЛУЧАЕМЫЙ РЕЗУЛЬТАТ
Требования законодательства Российской Федерации	**Определение возможных негативных последствий от реализации угроз безопасности информации**	Перечень возможных негативных последствий информации
Сведения о структурно-функциональных характеристиках информационной инфраструктуры		Информационные активы
Результаты оценки рисков		Виды неправомерного доступа и (или) воздействий
Сведения об информационных активах		Перечень угроз безопасности информации
Сведения о структурно-функциональных характеристиках информационной инфраструктуры	**Определениеусловий для реализации угроз безопасности информации**	Типы уязвимостей и (или) недекларированных возможностях
Сведения об уязвимостях		Варианты возможного доступа нарушителей информационной безопасности к объектам информационной инфраструктуры
Сведения о доступе к объектам информационной инфраструктуры		
Особенности организации банковских технологических процессов	**Определение источников угроз безопасности информации иоценку возможностей нарушителей**	Виды источников угроз безопасности информации
Сведения о сервисах, предоставляемых сторонними организациями		Возможные цели реализации угроз безопасности информации нарушителями
Сведения о типах внутренних и внешних пользователей.		Категории, виды и возможности нарушителей
Сведения об объектах информационной инфраструктуры и особенностях их функционирования	**Определение сценариев реализации угроз безопасности**	Перечень сценариев угроз безопасности информации

Условия реализации угроз безопасности информации	**информации**	
Категории, виды и возможности нарушителей		
Перечень сценариев реализации угроз безопасности информации	**Оценка уровня опасности угроз безопасности информации**	Уровни опасности угроз безопасности информации
Сведения о типе доступа к объектам информационной инфраструктуры		
Сведения о сложности реализации сценария		
Сведения об уровне значимости объектов информационной инфраструктуры		

Информационные активы Банка рассматриваются с учетом соответствующих объектов среды, где обеспечение информационной безопасности данных активов проявляется через установление необходимых мер защиты для соответствующих объектов среды. Процесс формирования перечней типов объектов среды осуществляется в соответствии с иерархией уровней информационной инфраструктуры Банка. При выявлении и классификации объектов среды в соответствии с иерархической структурой информационной инфраструктуры, банк может более точно определить необходимые меры безопасности, соответствующие уровню и важности каждого типа объекта в контексте общей информационной безопасности.

На каждом из уровней информационной инфраструктуры, приведенных в таблице 3, угрозы, указанные в таблице 4 и их источники, методы и средства защиты и подходы к оценке эффективности являются различными.

Таблица 3 – Иерархия уровней информационной инфраструктуры

Уровни информационной инфраструктуры	**Объекты среды**
Физический уровень	Физические носители информации, в составе системы хранения данных
	Физические носители информации, в составе системы резервного копирования
	Физические носители информации, в составе автоматизированных рабочих мест
	Съемные носители информации
	Каналы связи
	Мониторы
	Помещения/здания/сооружения
	Технические средства информационных систем
Сетевой уровень	Коммуникационное оборудование
Уровень сетевых приложений и сервисов	Сетевые приложения и сервисы
Уровень операционных	Файлы данных с информацией ограниченного распространения

систем	Общесистемные программные средства
	Информация, необходимая для идентификации, аутентификации и (или) авторизации
	Файлы данных с открытой информацией
Уровень систем управления базами данных	Базы данных информационных систем
	Информация, необходимая для идентификации, аутентификации и (или) авторизации
Уровень банковских технологических процессов и приложений	Программное обеспечение, предназначенное для обработки защищаемой информации
	Программное обеспечение, предназначенное для обработки открытой информации
	Информация, необходимая для идентификации, аутентификации и (или) авторизации
	Ключевые носители
	Бумажные документы
Уровень бизнес процессов	Информационные активы (сведения ограниченного доступа)
	Люди

Таблица 4 – Способы реализации угроз безопасности информации

Уровни информационной инфраструктуры	Способы реализации угроз
Физический уровень	**Хищение/кража**
	Утрата
	Уничтожение/разрушение
	Несанкционированный физический доступ
	Утечка видовой информации
	Утечка информации по каналам ПЭМИН
Сетевой уровень	**Атаки типа «отказ в обслуживании»**
	Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа
	Нарушение штатных режимов работы сетевого оборудования
	Внедрение аппаратных закладок
Уровень сетевых приложений и сервисов	**Внедрение вредоносного программного обеспечения**
	Анализ трафика
	Атаки типа «отказ в обслуживании»
	Использование специализированных программ
	Нарушение штатных режимов работы сетевых приложений
	Отказ от авторства
	Сканирование сети, направленное на выявление открытых портов и служб, открытых соединений
Уровень операционных систем	**Кража (утеря, компрометация) пароля**
	Копирование
	Модификация/удаление
	Нарушение штатных режимов работы ОС
	Распространение вредоносных программ
	Неправильное (не полное) конфигурирование СЗИ
	Несанкционированный доступ в ОС с использованием специализированного ПО
Уровень систем управления базамиданных	**Копирование**
	Неправильное (не полное) конфигурирование СЗИ
	Модификация/удаление
	Нарушение штатных режимов работы СУБД
	Подмена пользовательских идентификаторов
	Несанкционированный логический доступ к СУБД
	Распространение вредоносных программ
	Кража пароля
Уровень банковских технологических процессов и приложений	**Отказ от авторства**
	Модификация/удаление
	Распространение/передача
	Печать документов

	Нарушение штатных режимов работы приложений
	Кража документов и пластиковых карт
	Кража пароля
Уровень бизнес процессов	**Непреднамеренное нарушение бизнес-процесса**
	Преднамеренное нарушение бизнес-процесса

Все физические лица, имеющие доступ к техническим и программным средствам, разделяются на следующие категории:

− категория I – лица, не имеющие права доступа в помещения, где расположены технические и программные средства;

− категория II – лица, имеющие право постоянного или разового доступа в помещения, где расположены технические и программные средства.

Все потенциальные нарушители подразделяются на:

− внешних нарушителей, осуществляющих атаки вне пределов контролируемой зоны Банка;

− внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны Банка.

Таким образом, внешними нарушителями могут быть как лица категории I, так и лица категории II, а внутренними нарушителями могут быть только лица категории II.

Основные источники угроз безопасности информации приведены в таблице 5.

Таблица 5 – Перечень источников угроз безопасности информации

Типы источников угроз безопасности информации	Источники угроз безопасности информации
Компьютерные злоумышленники, осуществляющие целенаправленные деструктивные воздействия, в том числе использование компьютерных вирусов и других типов вредоносных	Хакер
	Компьютерный хулиган
Сотрудники Банка, являющиеся легальными участниками процессов в информационных системах и действующие в рамках предоставленных полномочий	Пользователи информационных систем
	Администраторы информационных систем
	Технический персонал, имеющий доступ к аппаратномуобеспечению
	Администраторы средств защиты информации
Сотрудники Банка, являющиеся легальными участниками процессов в информационных системах и действующие вне рамок предоставленных полномочий	Администраторы средств защиты информации
	Пользователи информационных систем
	Администраторы информационных систем
	Технический персонал, имеющий доступ к аппаратномуобеспечению
Неблагоприятные события природного и техногенного характера	Пожары
	Наводнения, землетрясения, извержения вулканов, ураганы,смерчи, тайфуны, цунами и т.д.
	Техногенные катастрофы
	Нарушение внутриклиматических условий
	Нарушение или снижение качества электропитания.
	Сбои и аварии в системах водоснабжения, канализации, отопления
Террористы, криминальные элементы	Террористы
	Криминальные элементы
	Недобросовестные конкуренты
Провайдеры	Провайдер канала связи
	Интернет-провайдер
Подрядчики, осуществляющие монтаж, пусконаладочные работы оборудования и его ремонт	Сотрудник технической поддержки
	Сервисный инженер
	Разработчик программного обеспечения
	Разработчик технических средств
Внешние нарушители, имеющиедоступ к ИС	Аудитор
	Партнер
	Клиент
	Сотрудник Надзорного ведомства

Таблица 6 – Возможные негативные последствия для ПАО ЗенитБанк

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
Причинение имущественного ущерба	АРМ главного инженера	Несанкционированная отправка команд, приводящая к несрабатыванию средств аварийной защиты и (или) к изменению логики
	АРМ оператора технической поддержки	Несанкционированная отправка команд, приводящая к несрабатыванию средств аварийной защиты и (или) к изменению логики
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.

Для выявления потенциальных нарушителей системы безопасности информации используются следующие исходные данные:

- Общий список угроз безопасности информации, предоставленный в банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru).

- Модели угроз безопасности информации, разрабатываемые ФСТЭК России в соответствии с установленными нормами.

- Отраслевые (ведомственные, корпоративные) модели угроз безопасности информации.

- Документация по сетям и системам, включающая информацию о структуре, архитектуре, группах пользователей, их полномочиях, типах доступа, а также внешних и внутренних интерфейсах.

- Оценка потенциальных отрицательных последствий от реализации угроз безопасности информации.

- Определение объектов воздействия угроз безопасности информации и видов воздействия на них.

На основе анализа этих исходных данных и результатов оценки возможных целей нарушителей формируется перечень актуальных нарушителей. В таблице 7 представлен перечень данных нарушителей.

Таблица 7 – Возможные нарушители и их цели для реализации угроз безопасности информации нарушителями

№ вида	Виды нарушителя	Категории нарушителя	Возможные цели реализации угроз ИБ
1	Преступные группы (мошенники, хакеры, шпионы)	Внешний	Получение финансовой или иной материальной выгоды. Дестабилизация деятельности Банка ЗенитБанк Не имеют достаточной мотивации для реализации угроз, однако рассматриваются, т.к. могут вступить в сговор с внутренними нарушителями
2	Конкурирующие организации	Внешний	Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды. Является возможным нарушителем, исходя из целей реализации угроз
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 Является возможным нарушителем, исходя из целей реализации угроз
4	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 Является возможным нарушителем, исходя из целей реализации угроз
5	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. Является возможным нарушителем, исходя из целей реализации угроз
6	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внутренний/Внешний	Получение финансовой или иной материальной выгоды. Непреднамеренные. Не имеют достаточной мотивации для реализации целей
7	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (охрана, уборщица)	Внутренний	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия Не имеют достаточной мотивации для реализации целей
8	Авторизованные пользователи систем и сетей	Внутренний	Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия. Является возможным нарушителем, исходя из целей реализации угроз

Нарушители демонстрируют различные уровни компетентности, наличия ресурсов и мотивацию для осуществления угроз безопасности информации. Эти характеристики, в совокупности, определяют уровень возможностей нарушителей в реализации угроз безопасности информации.

Определены следующие категории уровней возможностей нарушителей:

1) Нарушитель с базовыми возможностями по осуществлению угроз безопасности информации(У1)

2) Нарушитель с базовыми, но усиленными возможностями по реализации угроз безопасности информации(У2) .

3) Нарушитель с средним уровнем возможностей по реализации угроз безопасности информации(У3).

4) Нарушитель с высоким уровнем возможностей по реализации угроз безопасности информации(У4).

Однако, при сопоставлении данных из банка угроз безопасности информации возникает несоответствие с уровнями возможностей нарушителей, представленными в методическом документе "Методика оценки угроз безопасности информации". Таблица 8 демонстрирует расхождение в потенциале нарушителей между банком данных угроз и методическим документом.

Это расхождение подчеркивает необходимость пересмотра и согласования данных между различными источниками для более точной и надежной оценки уровней возможностей нарушителей в области информационной безопасности.

Таблица 8 - Соотношение потенциала нарушителей, в соответствии с банком данных угроз ФСТЭК

Банк данных угроз, сформированный ФСТЭК России	Методика оценки угроз безопасности информации
Нарушитель с низким потенциалом	Нарушитель с базовыми возможностями по осуществлению угроз безопасности информации.
	Нарушитель с базовыми, но усиленными возможностями по реализации угроз безопасности информации
Нарушитель со средним потенциалом	Нарушитель с средним уровнем возможностей по реализации угроз безопасности информации
Нарушитель с высоким потенциалом	Нарушитель с высоким уровнем возможностей по реализации угроз безопасности информации .

В зависимости от прав и условий доступа к системам и сетям, определенных архитектурой и режимами функционирования этих систем, а также учитывая возможности нарушителей, последние разделяются на две основные категории:

- Внешние нарушители, которые не обладают правами доступа в контролируемую (охраняемую) зону или полномочиями для доступа к информационным ресурсам и компонентам систем и сетей, требующим авторизации.

- Внутренние нарушители, которые, напротив, имеют соответствующие права доступа в контролируемую (охраняемую) зону и/или полномочия для автоматизированного доступа к информационным ресурсам и компонентам систем и сетей.

Эта дифференциация внешних и внутренних нарушителей основана на их возможностях проникновения в систему и уровне привилегий, что позволяет эффективнее разрабатывать стратегии и меры безопасности для противостояния угрозам. При этом важно учитывать, что уровень риска и необходимые меры безопасности могут различаться для каждой из указанных категорий нарушителей. В таблице оценка целей реализации

нарушителями угроз безопасности информации в зависимости от возможных негативных последствий и видов ущерба от их реализации

На основе проведенного сопоставления выявляются современные нарушители в соответствии с следующим критерием: нарушитель рассматривается как актуальный, если потенциальные цели его деятельности, направленной на осуществление угроз безопасности информации, могут иметь определенные негативные последствия для ПАО ЗенитБанк.

Этот принцип определения актуальных нарушителей позволяет выделить тех, чьи действия представляют наибольшую угрозу для безопасности информации банка. Идентификация таких нарушителей на ранних стадиях обеспечивает возможность принятия эффективных мер по предотвращению потенциальных угроз и минимизации возможных негативных последствий для организации. Возможные нарушители для Банка ПАО ЗенитБанк показаны в таблице 9.

Таблица 9 – Возможных нарушители

Виды риска / возможные негативные последствия*	Виды возможного нарушителя	Категория нарушителя	Уровень возможностей нарушителя
Нанесение ущерба физическому лицу	Преступные группы (мошенники, хакеры, шпионы)	Внешний	У3
	Конкурирующие организации	Внешний	У3
	Системные администраторы и администраторы безопасности	Внутренний	У2
	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внутренний	У2
	Авторизованные пользователи систем и сетей	Внутренний	У1
Нанесение ущерба юридическому лицу,	Преступные группы (мошенники, хакеры, шпионы)	Внешний	У3
	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний/ Внешний	У3
	Системные администраторы и администраторы безопасности	Внутренний	У2

Также в таблице 10 показана оценка целей реализации нарушителями угроз безопасности информации в зависимости от возможных негативных последствий и видов ущерба от их реализации

Таблица 10 – 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	
Преступные группы (мошенники, хакеры, шпионы)	+ (дестабилизация деятельности Банка)	У2 (утечка коммерческой тайны; причинение имущественного ущерба;)
Конкурирующие организации	+ (дестабилизация деятельности Банка)	У2 (невозможность заключения договоров;)
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, репутационный ущерб организации)

5. СПОСОБЫ РЕАЛИЗАЦИИ (ВОЗНИКНОВЕНИЯ) УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПАО ЗЕНИТ БАНК

В процессе оценки угроз безопасности информации выявляются потенциальные методы осуществления угроз безопасности информации. Эти методы могут быть использованы актуальными нарушителями для реализации угроз безопасности информации в информационной системе ПАО ЗенитБанк. В таблице 11 показаны актуальные способы реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности.

Таблица 11 – 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 (мошенники, хакеры, шпионы)**	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	**Разработчики**	Внутренний/	Доступ к базам данных	Веб-интерфейс удаленного	Использование уязвимостей

	программных, программно-аппаратных средств	Внешний		администрирования базы данных информационной системы Пользовательский веб-интерфейс доступа к базе данных информационной системы	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
4	**Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ**	Внутренний/ 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
			АРМ оператора	Съемные машинные носители информации, содержащие аутентификационную информацию	Извлечение аутентификационной информации из постоянной памяти носителя
5	**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

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 12.

Показатели, относящиеся к ИСПДн Банка ЗенитБанк выделены зеленым цветом .

Таблица 12 – 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 13 – Условия определения высокого уровня исходной защищенности

Технические и эксплуатационные характеристики	Уровень защищенности		
	Высокий	Средний	Низкий

ИСПДн			
ИТОГО	∑ ≥ 70%	∑ ≤ 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 14 – Условия определения среднего уровня исходной защищенности

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
ИТОГО	∑ < 70%	∑ ≥ 70%	∑ ≤ 30%

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

Таблица 15 – Условия определения низкого уровня исходной защищенности

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
ИТОГО	∑ < 70%	∑ < 70%	∑ > 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 16 – 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

7. ОПРЕДЕЛЕНИЕ АКТУАЛЬНЫХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПАО ЗЕНИТ БАНК

7.1. Идентификация угроз

В качестве исходных данных для определения угроз безопасности информации используется банк данных угроз безопасности информации (bdu.fstec.ru), ведение которого осуществляется ФСТЭК России в соответствии с подпунктом 21 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю.

7.2. Определение актуальности угроз безопасности информации

Перечень актуальных угроз безопасности информации ПАО Зенит Банк представлен в таблице 17.

Таблица 17 – Перечень актуальных угроз безопасности информации ПАО Зенит Банк

Номер угрозы	Наименование угроз	Вероятность (возможность) реализации угрозы	Степень возможного ущерба	Актуальность угрозы
УБИ. 003	Угроза анализа криптографических алгоритмов и их реализации	Высокая	Высокая	Актуальная
УБИ. 004	Угроза аппаратного сброса пароля BIOS	Высокая	Высокая	Актуальная
УБИ. 006	Угроза внедрения кода или данных	Высокая	Высокая	Актуальная
УБИ. 007	Угроза воздействия на программы с высокими привилегиями	Высокая	Высокая	Актуальная
УБИ. 008	Угроза восстановления и/или повторного использования аутентификационной информации	Высокая	Высокая	Актуальная
УБИ. 009	Угроза восстановления предыдущей уязвимой версии BIOS	Высокая	Высокая	Актуальная
УБИ. 010	Угроза выхода процесса за пределы виртуальной машины	Высокая	Высокая	Актуальная
УБИ. 012	Угроза деструктивного изменения конфигурации/среды окружения программ	Высокая	Высокая	Актуальная
УБИ. 013	Угроза деструктивного использования декларированного функционала BIOS	Высокая	Высокая	Актуальная
УБИ. 014	Угроза длительного удержания вычислительных ресурсов пользователями	Высокая	Высокая	Актуальная
УБИ. 015	Угроза доступа к защищаемым файлам с использованием обходного пути	Высокая	Высокая	Актуальная
УБИ. 016	Угроза доступа к локальным файлам сервера при помощи URL	Высокая	Высокая	Актуальная
УБИ. 017	Угроза доступа/перехвата/изменения HTTP cookies	Высокая	Высокая	Актуальная

Номер угрозы	Наименование угроз	Вероятность (возможность) реализации угрозы	Степень возможного ущерба	Актуальность угрозы
УБИ. 018	Угроза загрузки нештатной операционной системы	Высокая	Высокая	Актуальная
УБИ. 019	Угроза заражения DNS-кеша	Высокая	Высокая	Актуальная
УБИ. 022	Угроза избыточного выделения оперативной памяти	Высокая	Высокая	Актуальная
УБИ. 023	Угроза изменения компонентов информационной (автоматизированной) системы	Высокая	Высокая	Актуальная
УБИ. 025	Угроза изменения системных и глобальных переменных	Высокая	Высокая	Актуальная
УБИ. 026	Угроза искажения XML-схемы	Высокая	Высокая	Актуальная
УБИ. 027	Угроза искажения вводимой и выводимой на периферийные устройства информации	Высокая	Высокая	Актуальная
УБИ. 028	Угроза использования альтернативных путей доступа к ресурсам	Высокая	Высокая	Актуальная
УБИ. 030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Высокая	Высокая	Актуальная
УБИ. 031	Угроза использования механизмов авторизации для повышения привилегий	Высокая	Высокая	Актуальная
УБИ. 032	Угроза использования поддельных цифровых подписей BIOS	Высокая	Высокая	Актуальная
УБИ. 033	Угроза использования слабостей кодирования входных данных	Высокая	Высокая	Актуальная
УБИ. 034	Угроза использования слабостей протоколов сетевого/локального обмена данными	Высокая	Высокая	Актуальная
УБИ. 035	Угроза использования слабых криптографических алгоритмов BIOS	Высокая	Высокая	Актуальная

Номер угрозы	Наименование угроз	Вероятность (возможность) реализации угрозы	Степень возможного ущерба	Актуальность угрозы
УБИ. 036	Угроза исследования механизмов работы программы	Высокая	Высокая	Актуальная
УБИ. 037	Угроза исследования приложения через отчёты об ошибках	Высокая	Высокая	Актуальная
УБИ. 039	Угроза исчерпания запаса ключей, необходимых для обновления BIOS	Высокая	Высокая	Актуальная
УБИ. 041	Угроза межсайтового скриптинга	Высокая	Высокая	Актуальная
УБИ. 042	Угроза межсайтовой подделки запроса	Высокая	Высокая	Актуальная
УБИ. 044	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	Высокая	Высокая	Актуальная
УБИ. 045	Угроза нарушения изоляции среды исполнения BIOS	Высокая	Высокая	Актуальная
УБИ. 046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	Высокая	Высокая	Актуальная
УБИ. 048	Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин	Высокая	Высокая	Актуальная
УБИ. 049	Угроза нарушения целостности данных кеша	Высокая	Высокая	Актуальная
УБИ. 051	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	Высокая	Высокая	Актуальная
УБИ. 053	Угроза невозможности управления правами пользователей BIOS	Высокая	Высокая	Актуальная
УБИ. 059	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	Высокая	Высокая	Актуальная

Номер угрозы	Наименование угроз	Вероятность (возможность) реализации угрозы	Степень возможного ущерба	Актуальность угрозы
УБИ. 061	Угроза некорректного задания структуры данных транзакции	Высокая	Высокая	Актуальная
УБИ. 062	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	Высокая	Высокая	Актуальная
УБИ. 063	Угроза некорректного использования функционала программного и аппаратного обеспечения	Высокая	Высокая	Актуальная
УБИ. 067	Угроза неправомерного ознакомления с защищаемой информацией	Высокая	Высокая	Актуальная
УБИ. 068	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением	Высокая	Высокая	Актуальная
УБИ. 069	Угроза неправомерных действий в каналах связи	Высокая	Высокая	Актуальная
УБИ. 071	Угроза несанкционированного восстановления удалённой защищаемой информации	Высокая	Высокая	Актуальная
УБИ. 072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	Высокая	Высокая	Актуальная
УБИ. 073	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	Высокая	Высокая	Актуальная
УБИ. 074	Угроза несанкционированного доступа к аутентификационной информации	Высокая	Высокая	Актуальная
УБИ. 075	Угроза несанкционированного доступа к виртуальным каналам передачи	Высокая	Высокая	Актуальная
УБИ. 076	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	Высокая	Высокая	Актуальная

Номер угрозы	Наименование угроз	Вероятность (возможность) реализации угрозы	Степень возможного ущерба	Актуальность угрозы
УБИ. 077	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение	Высокая	Высокая	Актуальная
УБИ. 078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети	Высокая	Высокая	Актуальная
УБИ. 079	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин	Высокая	Высокая	Актуальная
УБИ. 080	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	Высокая	Высокая	Актуальная
УБИ. 084	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	Высокая	Высокая	Актуальная
УБИ. 085	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	Высокая	Высокая	Актуальная
УБИ. 086	Угроза несанкционированного изменения аутентификационной информации	Высокая	Высокая	Актуальная
УБИ. 087	Угроза несанкционированного использования привилегированных функций BIOS	Высокая	Высокая	Актуальная
УБИ. 088	Угроза несанкционированного копирования защищаемой информации	Высокая	Высокая	Актуальная
УБИ. 089	Угроза несанкционированного редактирования реестра	Высокая	Высокая	Актуальная
УБИ. 090	Угроза несанкционированного создания учётной записи пользователя	Высокая	Высокая	Актуальная
УБИ. 091	Угроза несанкционированного удаления защищаемой информации	Высокая	Высокая	Актуальная

Номер угрозы	Наименование угроз	Вероятность (возможность) реализации угрозы	Степень возможного ущерба	Актуальность угрозы
УБИ. 093	Угроза несанкционированного управления буфером	Высокая	Высокая	Актуальная
УБИ. 094	Угроза несанкционированного управления синхронизацией и состоянием	Высокая	Высокая	Актуальная
УБИ. 095	Угроза несанкционированного управления указателями	Высокая	Высокая	Актуальная
УБИ. 098	Угроза обнаружения открытых портов и идентификации привязанныхк ним сетевых служб	Высокая	Высокая	Актуальная
УБИ. 099	Угроза обнаружения хостов	Высокая	Высокая	Актуальная
УБИ. 100	Угроза обхода некорректно настроенных механизмов аутентификации	Высокая	Высокая	Актуальная
УБИ. 102	Угроза опосредованного управления группой программ через совместно используемые данные	Высокая	Высокая	Актуальная
УБИ. 103	Угроза определения типов объектов защиты	Высокая	Высокая	Актуальная
УБИ. 104	Угроза определения топологии вычислительной сети	Высокая	Высокая	Актуальная
УБИ. 108	Угроза ошибки обновления гипервизора	Высокая	Высокая	Актуальная
УБИ. 109	Угроза перебора всех настроек и параметров приложения	Высокая	Высокая	Актуальная
УБИ. 111	Угроза передачи данных по скрытым каналам	Высокая	Высокая	Актуальная
УБИ. 113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	Высокая	Высокая	Актуальная
УБИ. 114	Угроза переполнения целочисленных переменных	Высокая	Высокая	Актуальная

Номер угрозы	Наименование угроз	Вероятность (возможность) реализации угрозы	Степень возможного ущерба	Актуальность угрозы
УБИ. 115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	Высокая	Высокая	Актуальная
УБИ. 116	Угроза перехвата данных, передаваемых по вычислительной сети	Высокая	Высокая	Актуальная
УБИ. 117	Угроза перехвата привилегированного потока	Высокая	Высокая	Актуальная
УБИ. 118	Угроза перехвата привилегированного процесса	Высокая	Высокая	Актуальная
УБИ. 119	Угроза перехвата управления гипервизором	Высокая	Высокая	Актуальная
УБИ. 120	Угроза перехвата управления средой виртуализации	Высокая	Высокая	Актуальная
УБИ. 121	Угроза повреждения системного реестра	Высокая	Высокая	Актуальная
УБИ. 122	Угроза повышения привилегий	Высокая	Высокая	Актуальная
УБИ. 123	Угроза подбора пароля BIOS	Высокая	Высокая	Актуальная
УБИ. 124	Угроза подделки записей журнала регистрации событий	Высокая	Высокая	Актуальная
УБИ. 127	Угроза подмены действия пользователя путём обмана	Высокая	Высокая	Актуальная
УБИ. 128	Угроза подмены доверенного пользователя	Высокая	Высокая	Актуальная
УБИ. 129	Угроза подмены резервной копии программного обеспечения BIOS	Высокая	Высокая	Актуальная
УБИ. 130	Угроза подмены содержимого сетевых ресурсов	Высокая	Высокая	Актуальная
УБИ. 131	Угроза подмены субъекта сетевого доступа	Высокая	Высокая	Актуальная

Номер угрозы	Наименование угроз	Вероятность (возможность) реализации угрозы	Степень возможного ущерба	Актуальность угрозы
УБИ. 132	Угроза получения предварительной информации об объекте защиты	Высокая	Высокая	Актуальная
УБИ. 139	Угроза преодоления физической защиты	Высокая	Высокая	Актуальная
УБИ. 140	Угроза приведения системы в состояние «отказ в обслуживании»	Высокая	Высокая	Актуальная
УБИ. 143	Угроза программного выведения из строя средств хранения, обработкии (или) ввода/вывода/передачи информации	Высокая	Высокая	Актуальная
УБИ. 144	Угроза программного сброса пароля BIOS	Высокая	Высокая	Актуальная
УБИ. 145	Угроза пропуска проверки целостности программного обеспечения	Высокая	Высокая	Актуальная
УБИ. 149	Угроза сбоя обработки специальным образом изменённых файлов	Высокая	Высокая	Актуальная
УБИ. 150	Угроза сбоя процесса обновления BIOS	Высокая	Высокая	Актуальная
УБИ. 151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	Высокая	Высокая	Актуальная
УБИ. 152	Угроза удаления аутентификационной информации	Высокая	Высокая	Актуальная
УБИ. 153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	Высокая	Высокая	Актуальная
УБИ. 154	Угроза установки уязвимых версий обновления программного обеспечения BIOS	Высокая	Высокая	Актуальная
УБИ. 155	Угроза утраты вычислительных ресурсов	Высокая	Высокая	Актуальная
УБИ. 156	Угроза утраты носителей информации	Высокая	Высокая	Актуальная

Номер угрозы	Наименование угроз	Вероятность (возможность) реализации угрозы	Степень возможного ущерба	Актуальность угрозы
УБИ. 157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Высокая	Высокая	Актуальная
УБИ. 158	Угроза форматирования носителей информации	Высокая	Высокая	Актуальная
УБИ. 159	Угроза «форсированного веб-браузинга»	Высокая	Высокая	Актуальная
УБИ. 160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	Высокая	Высокая	Актуальная
УБИ. 162	Угроза эксплуатации цифровой подписи программного кода	Высокая	Высокая	Актуальная
УБИ. 163	Угроза перехвата исключения/сигнала из привилегированного блока функций	Высокая	Высокая	Актуальная
УБИ. 165	Угроза включения в проект не достоверно испытанных компонентов	Высокая	Высокая	Актуальная
УБИ. 166	Угроза внедрения системной избыточности	Высокая	Высокая	Актуальная
УБИ. 167	Угроза заражения компьютера при посещении неблагонадёжных сайтов	Высокая	Высокая	Актуальная
УБИ. 168	Угроза «кражи» учётной записи доступа к сетевым сервисам	Высокая	Высокая	Актуальная
УБИ. 169	Угроза наличия механизмов разработчика	Высокая	Высокая	Актуальная
УБИ. 170	Угроза неправомерного шифрования информации	Высокая	Высокая	Актуальная
УБИ. 171	Угроза скрытного включения вычислительного устройства в состав бот-сети	Высокая	Высокая	Актуальная
УБИ. 172	Угроза распространения «почтовых червей»	Высокая	Высокая	Актуальная

Номер угрозы	Наименование угроз	Вероятность (возможность) реализации угрозы	Степень возможного ущерба	Актуальность угрозы
УБИ. 173	Угроза «спама» веб-сервера	Высокая	Высокая	Актуальная
УБИ. 174	Угроза «фарминга»	Высокая	Высокая	Актуальная
УБИ. 175	Угроза «фишинга»	Высокая	Высокая	Актуальная
УБИ. 177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью	Высокая	Высокая	Актуальная
УБИ. 178	Угроза несанкционированного использования системных и сетевых утилит	Высокая	Высокая	Актуальная
УБИ. 179	Угроза несанкционированной модификации защищаемой информации	Высокая	Высокая	Актуальная
УБИ. 180	Угроза отказа подсистемы обеспечения температурного режима	Высокая	Высокая	Актуальная
УБИ. 181	Угроза перехвата одноразовых паролей в режиме реального времени	Высокая	Высокая	Актуальная
УБИ. 182	Угроза физического устаревания аппаратных компонентов	Высокая	Высокая	Актуальная
УБИ. 185	Угроза несанкционированного изменения параметров настройки средств защиты информации	Высокая	Высокая	Актуальная
УБИ. 186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	Высокая	Высокая	Актуальная
УБИ. 187	Угроза несанкционированного воздействия на средство защиты информации	Высокая	Высокая	Актуальная
УБИ. 188	Угроза подмены программного обеспечения	Высокая	Высокая	Актуальная
УБИ. 189	Угроза маскирования действий вредоносного кода	Высокая	Высокая	Актуальная

Номер угрозы	Наименование угроз	Вероятность (возможность) реализации угрозы	Степень возможного ущерба	Актуальность угрозы
УБИ. 190	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	Высокая	Высокая	Актуальная
УБИ. 191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Высокая	Высокая	Актуальная
УБИ. 192	Угроза использования уязвимых версий программного обеспечения	Высокая	Высокая	Актуальная
УБИ. 193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика	Высокая	Высокая	Актуальная
УБИ. 195	Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы	Высокая	Высокая	Актуальная
УБИ. 197	Угроза хищения аутентификационной информации из временных файлов cookie	Высокая	Высокая	Актуальная
УБИ. 198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов	Высокая	Высокая	Актуальная
УБИ. 201	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	Высокая	Высокая	Актуальная
УБИ. 205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты	Высокая	Высокая	Актуальная
УБИ. 208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	Высокая	Высокая	Актуальная
УБИ. 209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора	Высокая	Высокая	Актуальная

Номер угрозы	Наименование угроз	Вероятность (возможность) реализации угрозы	Степень возможного ущерба	Актуальностьугрозы
УБИ. 210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения	Высокая	Высокая	Актуальная
УБИ. 211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем	Высокая	Высокая	Актуальная
УБИ. 212	Угроза перехвата управления информационной системой	Высокая	Высокая	Актуальная
УБИ. 213	Угроза обхода многофакторной аутентификации	Высокая	Высокая	Актуальная
УБИ. 214	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	Высокая	Высокая	Актуальная
УБИ. 215	Угроза несанкционированного доступа к системе при помощи сторонних сервисов	Высокая	Высокая	Актуальная
УБИ. 217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения	Высокая	Высокая	Актуальная