УТВЕРЖДАЮ
Генеральный директор
ООО «Инновационные Финансовые Технологии»
_____ И.И. Иванов
«21» октября 2025 г.

МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Автоматизированной системы «Кредитный Конвейер» (АС «Кредитный Конвейер»)

г. Минск, 2025

Содержание

1. **Общие положения**
   - 1.1. Назначение и область применения документа
   - 1.2. Нормативно-правовая база
   - 1.3. Используемая методология
2. **Описание и характеристики объекта защиты**
   - 2.1. Назначение и архитектура АС «Кредитный Конвейер»
   - 2.2. Критичные информационные активы
   - 2.3. Информационные потоки и точки входа
3. **Описание негативных последствий**
   - 3.1. Последствия для субъектов персональных данных
   - 3.2. Последствия для ООО «ИФТ» (оператора)
   - 3.3. Последствия для государства
4. **Модель нарушителя**
   - 4.1. Внешний нарушитель
   - 4.2. Внутренний нарушитель
5. **Перечень актуальных угроз и сценариев их реализации**
   - 5.1. Сценарий №1: Целевая атака с использованием программы-вымогателя
   - 5.2. Сценарий №2: Хищение базы данных клиентов с целью продажи
6. **Оценка актуальности угроз**
7. **Связь угроз с мерами и средствами защиты**
8. **Порядок пересмотра и актуализации модели угроз**

Приложение А: Функциональная схема АС «Кредитный Конвейер»
Приложение Б: Тепловая карта покрытия техник MITRE ATT&CK

---

1. Общие положения
1.1. Назначение и область применения документа

Настоящая Модель угроз безопасности информации (далее – Модель угроз) разработана для автоматизированной системы «Кредитный Конвейер» (далее – АС «Кредитный Конвейер» или Система) Общества с ограниченной ответственностью «Инновационные Финансовые Технологии» (далее – ООО «ИФТ»).

Документ устанавливает перечень актуальных угроз безопасности информации, обрабатываемой в Системе, описывает возможные сценарии их реализации, модель потенциального нарушителя и является основой для формирования Технического задания на создание системы защиты информации и разработки организационно-распорядительной документации.

1.2. Нормативно-правовая база

- Закон Республики Беларусь от 10.11.2008 № 455-З «Об информации, информатизации и защите информации».
- Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 10.12.2024 № 259.
- СТБ 34.101.30-2017 «Информационные технологии и безопасность. Методы и средства безопасности. Классификация информационных систем».

1.3. Используемая методология

Настоящая Модель угроз разработана с учетом требований Положения о порядке аттестации систем защиты информации. Для идентификации, классификации и детализации способов и техник реализации атак используется база знаний **MITRE ATT&CK for Enterprise v15**, как наиболее полная и признанная в международной практике. При документировании угроз приводится сопоставление с каталогом угроз безопасности информации ФСТЭК России для обеспечения соответствия подходам регулятора.

2. Описание и характеристики объекта защиты
2.1. Назначение и архитектура АС «Кредитный Конвейер»

АС «Кредитный Конвейер» предназначена для автоматизации процесса рассмотрения и выдачи онлайн-займов для субъектов малого и среднего предпринимательства. Система отнесена к классу **3-юл** (обработка коммерческой тайны) и **3-ин** (обработка персональных данных).

Архитектура Системы включает три основных компонента:

- **Веб-сервер:** Обрабатывает запросы от пользователей через публичный веб-интерфейс, расположен в демилитаризованной зоне (DMZ).
- **Сервер приложений:** Реализует бизнес-логику системы, включая скоринговую модель. Расположен во внутренней сети.
- **Сервер баз данных (СУБД):** Хранит всю информацию о клиентах, заявках и договорах. Расположен в защищенном сегменте внутренней сети.

2.2. Критичные информационные активы

1. **Персональные данные клиентов:** ФИО, паспортные данные, контактная информация, сведения о финансовом положении.
2. **Коммерческая тайна ООО «ИФТ»:** Алгоритмы скоринговой модели, внутренняя финансовая отчетность.
3. **Данные о заявках и договорах:** Информация о суммах, сроках и условиях займов, являющаяся банковской и коммерческой тайной клиентов.

2.3. Информационные потоки и точки входа

- **Внешние точки входа:**
  - Веб-интерфейс для клиентов (https://credit.ift.by).
  - Корпоративный почтовый сервер.
  - VPN-шлюз для удаленного доступа администраторов.
- **Внутренние точки входа:**
  - АРМ сотрудников кредитного отдела, имеющих доступ к серверу приложений.
  - АРМ администраторов Системы.

3. Описание негативных последствий

3.1. Последствия для субъектов персональных данных

Реализация угроз может привести к утечке персональных и финансовых данных клиентов, что повлечет за собой их использование в мошеннических схемах, финансовые потери и нарушение их законных прав и свобод.

3.2. Последствия для ООО «ИФТ» (оператора)

- **Прямой финансовый ущерб:** Хищение средств, выплата выкупа злоумышленникам, штрафы регуляторов (Национальный банк, ОАЦ).
- **Репутационный ущерб:** Потеря доверия клиентов и партнеров, снижение рыночной доли.
- **Операционный ущерб:** Приостановка основной деятельности (выдачи займов) из-за нарушения работоспособности Системы.

3.3. Последствия для государства

Нарушение стабильности финансового сектора в случае массового инцидента, подрыв доверия граждан к цифровым финансовым услугам.

4. Модель нарушителя

4.1. Внешний нарушитель (средний потенциал)

- **Мотивация:** Финансовая выгода (продажа данных, вымогательство), промышленный шпионаж.
- **Осведомленность:** Осведомлен об общедоступной информации о компании, может проводить активную разведку.
- **Инструментарий:** Использует общедоступные и коммерческие инструменты для сканирования, эксплуатации уязвимостей (Metasploit),

социальной инженерии. Может являться членом киберпреступной группировки.
- **Точки доступа:** Публичный веб-интерфейс, корпоративная почта.

4.2. Внутренний нарушитель (низкий/средний потенциал)
- **Мотивация:** Непреднамеренные действия (ошибки, переход по фишинговым ссылкам), личная неприязнь, финансовая выгода (продажа данных конкурентам).
- **Осведомленность:** Обладает знаниями о внутренней структуре сети, бизнес-процессах и используемом ПО. Имеет легальный доступ к сегментам сети.
- **Инструментарий:** Использует штатные средства ОС, легитимные учетные данные. Может использовать простые вредоносные скрипты.
- **Точки доступа:** Рабочие станции (АРМ).

5. Перечень актуальных угроз и сценариев их реализации
5.1. Сценарий №1: Целевая атака с использованием программы-вымогателя
- **Цель нарушителя:** Шифрование базы данных клиентов и серверов для получения выкупа.
- **Описание:** Внешний нарушитель проникает в сеть через фишинговое письмо, закрепляется в системе, повышает привилегии, распространяется на сервер СУБД и шифрует критичные данные.

Тактика (MITRE ATT&CK)	**Техника (MITRE ATT&CK)**	**Описание реализации в АС «Кредитный Конвейер»**	**Соответствие ФСТЭК/ОАЦ**
Initial Access	**T1566.002: Spearphishing Link**	Сотрудник кредитного отдела получает письмо, замаскированное под запрос от регулятора, со ссылкой на вредоносный сайт, с которого загружается ВПО.	УБИ.123
Execution	**T1204.002: Malicious File**	Сотрудник открывает загруженный файл (например, .docm с макросом), инициируя выполнение вредоносного кода.	УБИ.078
Persistence	**T1053.005: Scheduled Task**	ВПО создает задачу в Планировщике заданий Windows для обеспечения автозапуска после перезагрузки АРМ.	УБИ.105

Credential Access	**T1003.001: LSASS Memory**	ВПО использует инструмент типа Mimikatz для извлечения хэшей паролей из памяти процесса LSASS на скомпрометированном АРМ.	УБИ.031
Lateral Movement	**T1021.001: Remote Desktop Protocol**	Используя похищенные учетные данные администратора, нарушитель подключается по RDP к серверу приложений.	УБИ.098
Impact	**T1486: Data Encrypted for Impact**	С сервера приложений нарушитель получает доступ к серверу СУБД и запускает шифровальщик, который шифрует файлы базы данных.	УБИ.041

5.2. Сценарий №2: Хищение базы данных клиентов с целью продажи

- **Цель нарушителя:** Эксфильтрация (вывод) базы данных клиентов для последующей продажи на теневых форумах.
- **Описание:** Внешний нарушитель эксплуатирует уязвимость в веб-приложении, получает доступ к СУБД, собирает данные и скрытно выводит их из периметра.

Тактика (MITRE ATT&CK)	**Техника (MITRE ATT&CK)**	**Описание реализации в АС «Кредитный Конвейер»**	**Соответствие ФСТЭК/ОАЦ**
Initial Access	**T1190: Exploit Public-Facing Application**	Нарушитель находит и эксплуатирует уязвимость типа SQL-инъекция в форме авторизации на сайте credit.ift.by.	УБИ.081
Discovery	**T1046: Network Service Discovery**	Получив доступ к веб-серверу, нарушитель сканирует внутреннюю сеть для обнаружения сервера СУБД (порт 5432 для PostgreSQL).	УБИ.064

Collection	**T1005: Data from Local System**	Нарушитель выполняет прямые SQL-запросы к базе данных для извлечения таблиц с персональными данными клиентов и формирования дампа.	УБИ.017
Command & Control	**T1071.001: Web Protocols (HTTPS)**	Для управления и передачи данных нарушитель использует скрытый канал связи, маскируя трафик под легитимный HTTPS-трафик к своему C2-серверу.	УБИ.024
Exfiltration	**T1041: Exfiltration Over C2 Channel**	Дамп базы данных передается по установленному C2-каналу на сервер злоумышленника.	УБИ.070
Defense Evasion	**T1070.004: File Deletion**	Для сокрытия следов нарушитель удаляет временные файлы (дамп БД) и очищает логи веб-сервера.	УБИ.051

6. Оценка актуальности угроз

Угроза признается актуальной, если для нее существует хотя бы один реалистичный сценарий, соответствующий модели нарушителя и приводящий к значимым негативным последствиям.

Угроза (обобщенно)	**Сценарий**	**Вероятность реализации**	**Потенциальный ущерб**	**Статус**
Заражение ВПО-шифровальщиком	Сценарий №1	**Высокая**	**Критический**	**АКТУАЛЬНА**
Несанкционированный доступ к ПДн	Сценарий №2	**Средняя**	**Высокий**	**АКТУАЛЬНА**

Внедрение аппаратных закладок	Требует физического доступа на этапе поставки. Не соответствует модели нарушителя.	**Низкая**	**Критический**	**НЕ АКТУАЛЬНА**

7. Связь угроз с мерами и средствами защиты

Ниже представлена таблица соответствия актуальных техник атак внедряемым мерам и средствам защиты и обнаружения.

Техника (MITRE ATT&CK)	**Мера защиты (Противодействие)**	**Метод обнаружения**	**Внедряемое решение**
T1566.002: Spearphishing Link	Обучение пользователей; Фильтрация почты; Песочница для ссылок.	Анализ заголовков почты; Срабатывание правил на шлюзе безопасности; Оповещения от пользователей.	Email Security Gateway; Программы повышения осведомленности.
T1003.001: LSASS Memory	Изоляция учетных данных (Credential Guard); Защита процессов LSA.	Мониторинг доступа к процессу lsass.exe; Поведенческий анализ EDR.	Endpoint Detection and Response (EDR) с модулем защиты памяти.
T1190: Exploit Public-Facing Application	Анализ защищенности кода (SAST/DAST); Валидация входных данных.	Мониторинг логов; Правила корреляции на аномальные SQL-запросы.	Web Application Firewall (WAF); SIEM-система.
T1041: Exfiltration Over C2 Channel	Анализ сетевого трафика (DPI); Блокировка C2-серверов по репутационным спискам.	Обнаружение аномалий в сетевом трафике (объем, регулярность); Мониторинг DNS-запросов.	Межсетевой экран нового поколения (NGFW); Network Traffic Analysis (NTA).

8. Порядок пересмотра и актуализации модели угроз

Настоящая Модель угроз подлежит обязательному пересмотру и актуализации в следующих случаях:

- Планово – не реже одного раза в год.
- Внепланово – при значительных изменениях в архитектуре АС «Кредитный Конвейер», появлении новых векторов атак или по результатам расследования инцидентов ИБ.

Документ разработан:
Начальник отдела ИБ
ООО «ИФТ» _____ А.П. Сидоров