**Модель угроз АО «Банк Акционерный Кредитный Стабильный»**

**1. Описание информационных активов**

АО «Банк Акционерный Кредитный Стабильный» использует следующие ключевые информационные активы:

 **Серверы приложений и баз данных**

* **Назначение**: Обработка данных клиентов, выполнение транзакций, хранение данных.
* **Возможные виды воздействия**:
  + Несанкционированный доступ к данным.
  + Нарушение целостности данных.
  + Отказ в обслуживании.

 **Сеть передачи данных**

* **Назначение**: Обеспечение передачи данных между филиалами, банкоматами, клиентами и головным офисом.
* **Возможные виды воздействия**:
  + Перехват данных в сети (атака типа "человек посередине").
  + Нарушение целостности данных при передаче.
  + Снижение производительности сети.

 **Интернет-банк и мобильное приложение**

* **Назначение**: Предоставление удаленного доступа клиентам к банковским услугам.
* **Возможные виды воздействия**:
  + Несанкционированный доступ к учетным записям клиентов.
  + Фишинг и кража учетных данных.
  + Нарушение конфиденциальности клиентских данных.

 **Система управления доступом**

* **Назначение**: Контроль доступа сотрудников и клиентов к системам банка.
* **Возможные виды воздействия**:
  + Эскалация привилегий.
  + Компрометация учетных данных.
  + Угроза отказа в обслуживании (DoS).

 **Платежные системы**

* **Назначение**: Обработка и проведение внутренних и международных транзакций.
* **Возможные виды воздействия**:
  + Нарушение целостности транзакций.
  + Подмена транзакций или их отмена.
  + Несанкционированный доступ и манипуляции с платежами.

**2. Определение угроз**

| **Угроза** | **Источник** | **Пример угрозы** |
| --- | --- | --- |
| Несанкционированный доступ | Внешние и внутренние | Киберпреступники, сотрудники |
| Вредоносное ПО | Внешние | Вирусы, трояны, программы-вымогатели |
| Атака на веб-приложение | Внешние | SQL-инъекция, XSS (межсайтовый скриптинг) |
| Утечка конфиденциальной информации | Внутренние | Инсайдерская угроза, ошибка сотрудника |
| Фишинг | Внешние | Фальшивые письма для получения данных клиента |
| DDoS-атака | Внешние | Перегрузка серверов банка, нарушение доступности |
| Эксплуатация уязвимостей системы | Внешние и внутренние | Использование неизвестных уязвимостей (0-day) |
| Нарушение целостности данных | Внутренние | Умышленное или случайное изменение данных |
| Физический доступ к серверному оборудованию | Внешние и внутренние | Несанкционированный доступ в серверное помещение |

**3. Источники угроз**

1. **Внешние злоумышленники (киберпреступники)**
   * **Возможности**: Использование вредоносного ПО, проведение фишинговых атак, эксплуатация уязвимостей в системах удаленного доступа.
   * **Цели**: Кража финансовых данных клиентов, вымогательство (например, с помощью программ-вымогателей), нарушение доступности сервисов (DDoS-атаки).
2. **Инсайдеры (сотрудники и подрядчики)**
   * **Возможности**: Доступ к конфиденциальным данным, привилегированный доступ к системам, возможность саботажа или утечки информации.
   * **Цели**: Личное обогащение, месть, корпоративный шпионаж, нарушение работы ключевых сервисов.
3. **Конкуренты**
   * **Возможности**: Использование инсайдеров, кибершпионаж, атаки через компрометированных поставщиков или подрядчиков.
   * **Цели**: Получение конкурентных преимуществ, кража данных для использования в своих целях, дискредитация банка.
4. **Хактивисты**
   * **Возможности**: Организация DDoS-атак, взлом веб-сайтов банка для публичной дискредитации, раскрытие данных с целью воздействия на репутацию.
   * **Цели**: Протесты против политики банка, публичная дискредитация, кража и публикация данных в открытом доступе.
5. **Нарушители, использующие физический доступ**
   * **Возможности**: Кража серверного оборудования, внедрение шпионского ПО через физический доступ, манипуляция физическими устройствами (например, банкоматы).
   * **Цели**: Кража конфиденциальных данных, получение доступа к системе, выведение из строя оборудования.

#### Возможности и средства нарушителей

* **Технические средства**: Вредоносное ПО, инструменты для атаки на веб-приложения (например, Metasploit), DDoS-ботнеты, социальная инженерия.
* **Программные возможности**: Скрипты для перехвата данных, инструменты для фишинговых атак, программные средства для анализа сетевого трафика.
* **Физические возможности**: Доступ к серверным помещениям, подключение к корпоративной сети через физические порты, атаки на оборудование в публичных местах (например, банкоматы).

**4. Уязвимости**

* Слабые пароли или отсутствие двухфакторной аутентификации.
* Отсутствие обновлений систем безопасности, которые оставляют уязвимости незащищенными.
* Недостаточный контроль за сетевыми соединениями и трафиком.
* Отсутствие шифрования чувствительных данных.
* Недостаточное обучение сотрудников по вопросам информационной безопасности.

**5. Риски и угрозы**

| **Угроза** | **Источник** | **Пример угрозы** | **Уязвимость** | **Вероятность** | **Влияние** | **Риск** | **Меры по снижению риска** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Социальная инженерия | Внешние | Злоумышленники получают доступ через обман | Недостаточное обучение сотрудников | Высокая | Высокое | Высокий | Обучение, тесты на осведомленность сотрудников |
| Компрометация учетных данных | Внешние и внутренние | Утечка или кража учетных данных | Слабые пароли, отсутствие шифрования | Высокая | Высокое | Высокий | MFA, строгая политика паролей, регулярная смена |
| Целевая атака (APT) | Внешние | Долгосрочная целевая атака | Отсутствие специализированного мониторинга | Низкая | Высокое | Средний | Мониторинг, обнаружение аномалий, сетевые сегменты |
| Компрометация поставщиков | Внешние | Поставщики ИТ-систем становятся угрозой | Недостаточные проверки подрядчиков | Средняя | Высокое | Высокий | Проверка подрядчиков, сегментация |
| Внутреннее мошенничество | Внутренние | Сотрудники злоупотребляют полномочиями | Слабый контроль привилегий | Средняя | Высокое | Высокий | Мониторинг действий, ограничение прав доступа |
| Перехват данных в сети | Внешние | Атаки типа "человек посередине" (MITM) | Отсутствие шифрования сетевого трафика | Высокая | Высокое | Высокий | SSL/TLS, шифрование, обнаружение атак |
| Угроза отказа от обслуживания внутренних систем | Внутренние | Ошибки системных администраторов | Слабый контроль изменений | Низкая | Среднее | Средний | Политика изменений, резервные системы |
| Саботаж со стороны сотрудников | Внутренние | Умышленное повреждение данных | Недостаточный контроль привилегий | Низкая | Высокое | Средний | Логирование, мониторинг действий |
| Недостаток резервного копирования | Внешние и внутренние | Потеря данных из-за отсутствия копий | Отсутствие системы резервного копирования | Средняя | Высокое | Высокий | Регулярное резервное копирование |
| Уязвимости сторонних приложений | Внешние | Использование сторонних приложений | Отсутствие тестирования на уязвимости | Средняя | Среднее | Средний | Пентесты, оценка сторонних приложений |
| Кража устройств с конфиденциальными данными | Внутренние | Потеря ноутбуков или смартфонов | Отсутствие шифрования на устройствах | Низкая | Высокое | Средний | Шифрование, удаленное стирание данных |
| Нарушение конфиденциальности через ошибочные действия | Внутренние | Отправка данных неверным получателям | Низкий контроль за отправкой | Средняя | Среднее | Средний | Политика передачи данных, DLP-системы |
| Злоупотребление привилегиями | Внутренние | Сотрудники используют привилегии в личных целях | Недостаточный контроль доступа | Средняя | Высокое | Высокий | Логирование и мониторинг действий |
| Нарушение конфиденциальности из-за утечек API | Внешние | Уязвимости в API | Недостаточный контроль доступа к API | Высокая | Высокое | Высокий | Аутентификация, токены, мониторинг |
| Манипуляции с данными для мошенничества | Внутренние | Сотрудники подделывают данные для выгоды | Недостаточный контроль за целостностью данных | Средняя | Высокое | Высокий | Контроль изменений, анализ аномалий |

### Меры по снижению рисков

1. **Социальная инженерия**: Регулярное обучение сотрудников и моделирование фишинговых атак для повышения осведомленности.
2. **Компрометация учетных данных**: Использование средств двухфакторной аутентификации и периодическая смена паролей.
3. **Целевая атака (APT)**: Внедрение средств для обнаружения аномалий в трафике и событий, регулярный анализ логов.
4. **Компрометация поставщиков**: Проведение оценки безопасности поставщиков и ограничение их доступа.
5. **Перехват данных в сети**: Настройка шифрования для всех сетевых соединений и использование средств обнаружения атак.
6. **Саботаж сотрудников**: Мониторинг действий сотрудников с привилегиями, раздельные права доступа.
7. **Резервное копирование**: Внедрение системы регулярного резервного копирования с возможностью восстановления.
8. **Уязвимости сторонних приложений**: Проведение пентестов и регулярного сканирования на уязвимости всех приложений.
9. **Кража устройств**: Шифрование данных на мобильных устройствах и возможность их удаленного стирания.
10. **Нарушение конфиденциальности через ошибочные действия**: Внедрение системы предотвращения утечек данных (DLP).
11. **Злоупотребление привилегиями**: Политика минимальных привилегий и мониторинг действий с привилегиями.
12. **Уязвимости API**: Усиленная аутентификация для доступа к API, контроль доступа и мониторинг аномалий.
13. **Манипуляции с данными**: Внедрение контроля целостности данных и анализа аномалий в действиях с данными.

Эта модель угроз для АО «Банк Акционерный Кредитный Стабильный» охватывает основные потенциальные угрозы, уязвимости и риски, с которыми может столкнуться финансовая организация, и предлагает соответствующие меры защиты. Модель можно адаптировать под более специфические сценарии или расширить в зависимости от потребностей и особенностей финансовой организации.