

Защита банкоматов

Цель работы:

Классификация преступлений против АТМ-устройств, а также методы борьбы с ними.

Создание комплексной защиты банкоматов с минимальными затратами.

Выполнили

Ученик ГБПОУ «1-й МОК»:

Саркисян А.О.

Научный руководитель:

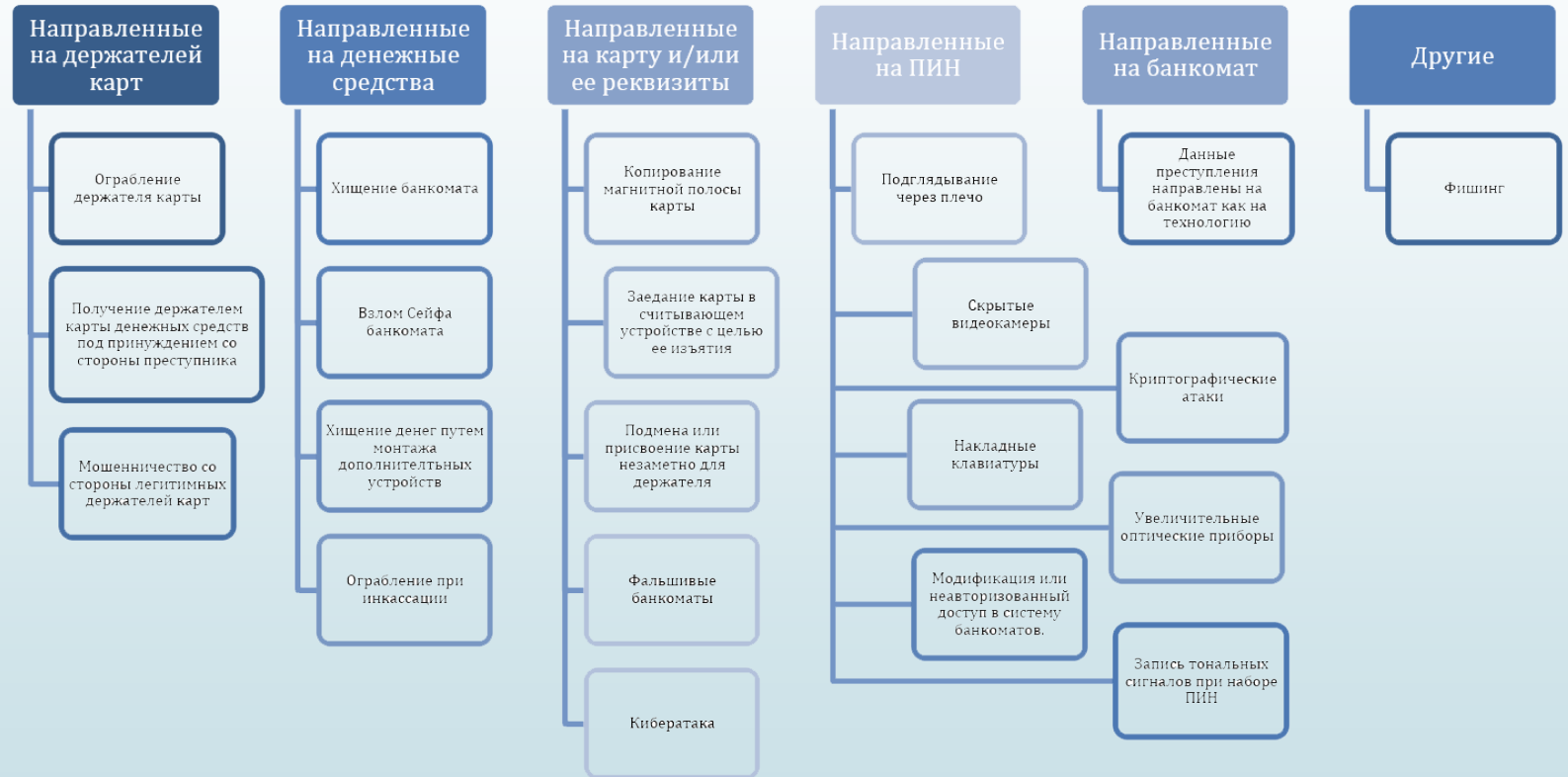
Козулина Ю.В.

Задачи, которые были выполнены в ходе работы

- Был проведен анализ по наиболее распространенным формам преступления против АТМ-устройств.
- Были проанализированы методы защиты против основных форм преступлений.
- Была составлена сравнительная таблица, учитывающая особенности различных форм атак и защит.
- Была создана программа, позволяющая в автоматическом и ручном режиме создать комплексную защиту банкоматов, в рамках фиксированного бюджета.

Основные виды атак

- Существует более 20-ти способов банкоматного мошенничества.
- Более 50% атак нацелены на банкомат, как на физическое устройство.
- Лишь около 10% атак, используют виртуальную уязвимость банкомата.



Направленные на держателей карт

- ▶ Угрозы, направленные непосредственно на человека. Он может быть ограблен, запуган или обманут. Порой в качестве мошенника выступает сам держатель карты.



Направленные на денежные средства

- ▶ Угрозы направленные на банкомат, как на физическое устройство. Сюда входят: взломы, кражи, ограбления при перевозке и монтаж дополнительных устройств.



Направленные на карту

- Использование различных устройств с целью кражи данных с карты, присвоения карты и пр. для дальнейшего использования этих данных для получения денежных средств.



Направленные на ПИН

- ▶ Уловки, выполняющиеся устройством или, непосредственно мошенником с целью получения ПИН-кода.



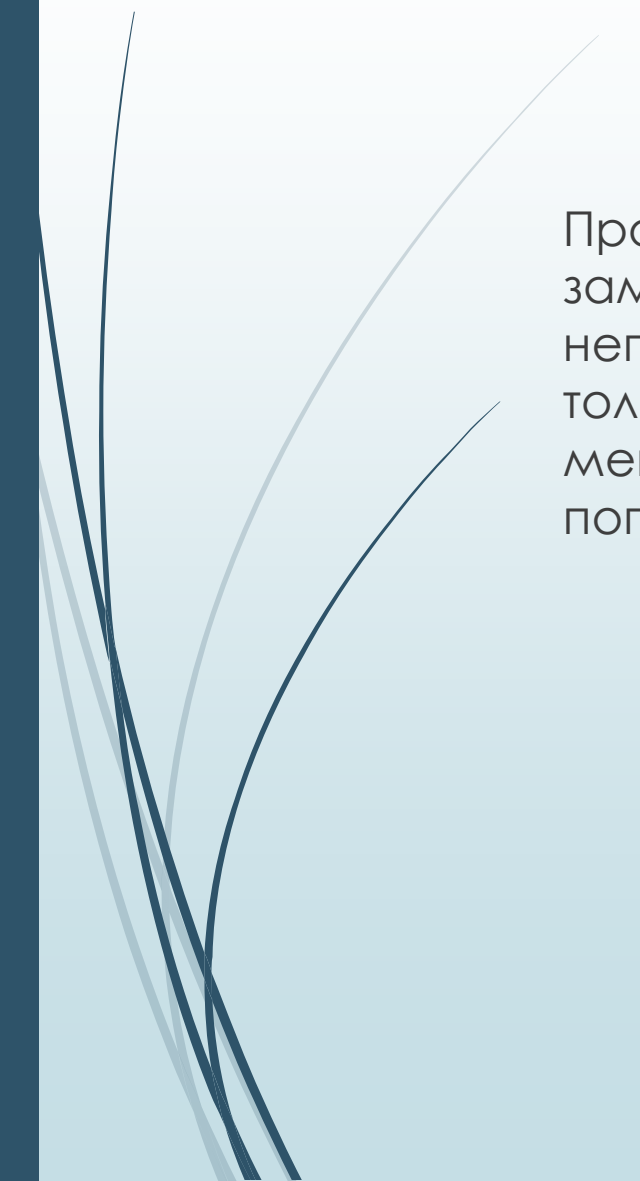
Другие

- ▶ Одним из примеров является фишинг. Способ, направленный на получение данных с карты путем массовой рассылки под именем популярных брендов.





Вывод по атакам



Проанализировав данные методы банкоматного мошенничества, можно заметить, что почти во всех видах мошенничества преступник находится в непосредственной близости от атакуемого объекта. Однако защищаться только физически тоже нельзя, так как есть и другие угрозы, пусть и в меньшей степени. Для защиты существует множество методов, давайте попробуем в них разобраться.

Современные методы защиты

Сигнализация



Защищает от:

- угроз направленных на держателей карт.
- физических атак на банкоматы.
- накладных устройств .
- направленных на кражу карты.

Видеонаблюдение



Защищает от:

- угроз направленных на держателей карт.
- атак на банкоматы.
- ограбление инкассации.
- направленных на кражу карты.
- получения данных с карты.
- подглядывания.
- накладных устройств.

Программы защиты



Защищает от:

- накладных устройств.
- кибератак.

Аналитический отдел

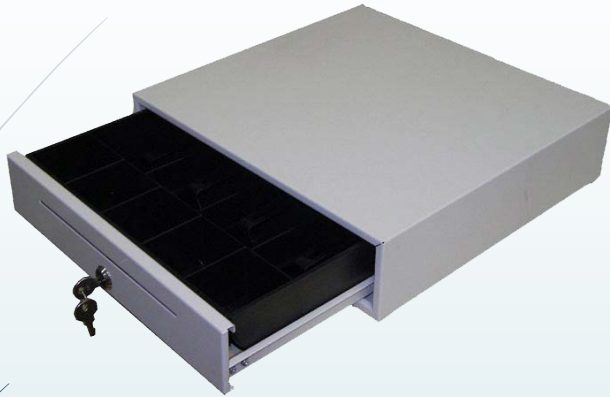


Защищает от:

- мошенничества со стороны легитимных владельцев
- кибератак

Современные методы защиты

Спец. Контейнеры



Защищает от:

- атака на банкомат.
- ограбление инкассации.

АНТИСКИММИНГ



Защищает от:

- направленных на кражу карты.
- направленных на получение данных с карты.
- накладных устройств.

Итоговая таблица

	Направленные на держателей карт	Мошенничество со стороны легитимных владельцев	Атака на банкоматы	Ограбление инкассации	Направленные на кражу карты	Направленные на получение данных с карты	Подглядывание	Накладные устройства	Кибератаки
Сигнализация	Полная защита	Отсутствие защиты	Полная защита	Отсутствие защиты	Полная защита	Отсутствие защиты	Отсутствие защиты	Возможность защиты	Отсутствие защиты
Электронные программы защиты	Отсутствие защиты	Отсутствие защиты	Отсутствие защиты	Отсутствие защиты	Отсутствие защиты	Отсутствие защиты	Отсутствие защиты	Возможность защиты	Полная защита
Видео-наблюдение	Полная защита	Отсутствие защиты	Полная защита	Полная защита	Полная защита	Возможность защиты	Возможность защиты	Возможность защиты	Отсутствие защиты
Спец. контейнеры	Отсутствие защиты	Отсутствие защиты	Полная защита	Полная защита	Отсутствие защиты	Отсутствие защиты	Отсутствие защиты	Отсутствие защиты	Отсутствие защиты
Антискимминг	Отсутствие защиты	Отсутствие защиты	Отсутствие защиты	Отсутствие защиты	Полная защита	Возможность защиты	Отсутствие защиты	Полная защита	Отсутствие защиты
Аналитический отдел	Отсутствие защиты	Полная защита	Отсутствие защиты	Отсутствие защиты	Отсутствие защиты	Отсутствие защиты	Отсутствие защиты	Отсутствие защиты	Полная защита

- **Возможность защиты**
- **Полная защита**
- **Отсутствие защиты**

Наша компьютерная программа

Возможности программы:

- ▶ Подборка комплексной защиты на основе фиксированного бюджета.
- ▶ Выдача готового решения для защиты банкомата на основе диапазона бюджета.
- ▶ Сборка собственного решения с параллельным выводом стоимости.
- ▶ Учет уязвимостей защиты, возможность улучшения отдельных пунктов защиты.
- ▶ Постоянный мониторинг слабых звеньев в системе.

Мои Настройки

	Направление на	Мощность со	Атака на банкомат	Обработка заявок	Направление на	Направление на	Подглядывание	Накладные устрой	Кибератаки
Сигнализация	1	0	1	0	1	0	0	0	0
Электронная сист	0	0	0	0	0	0	0	0	1
Видеонаблюдение	1	0	1	1	1	0	0	0	0
Специальные меры	0	0	1	1	0	0	0	0	0
Детектирование	0	0	0	0	1	0	0	1	0
Анализировать от	0	1	0	0	0	0	0	0	1

Стоймость текущей конфигурации: 0 Euro

Label



Итог

Данная комплексная система мер по защите банкоматов разрабатывалась с учетом всех озвученных выше условий: рентабельности, качества защиты и возможности быстро реагировать на изменение внешней среды. Нам удалось проделать работу, которая позволит облегчить поиски нужной защиты для предприятия.



Спасибо за внимание

