Модель угроз безопасности ПАО Сбербанк

Аннотация

Экономическая обстановка 1970-1980-х годах создала идеальные условия для банковского кризиса, что привело к неспособности банков выполнять свои обязательства перед клиентами. Указанные события показали необходимость создания единых требований к собственному капиталу банков. Такие требования разработаны Базельским комитетом по банковскому надзору. В 2004 году Базельским комитетом принят документ, содержащий требования к капиталу под операционный риск (риск возникновения прямых и непрямых потерь в результате несовершенства или ошибочных внутренних процессов кредитной организации, действий персонала и иных лиц, сбоев и недостатков информационных, технологических и иных систем, а также в результате реализации внешних событий).

Банки с 2004 года внедряют и используют комплексные подходы по управлению операционным риском, но международные требования, находящиеся в основе системы управления операционным риском не учитывают российских особенностей.

Чистая прибыль Сбера в 2023 году в размере 1,5 трлн руб. является подтверждением качества бизнес-модели, процессного, операционного и риск управления, которое отражается на качестве портфеля банка. Однако, до 2021 года сумма убытка банка от операционного риска росла на 20% ежегодно.

Факторный анализ показал влияние на рост реализованного операционного риска, инцидентов, источником возникновения которых является внешнее мошенничество. Указанные события Базельским комитетом не выделены в отдельный вид операционного риска, но существующие реалии требуют формирования Риска безопасности.

В рамках масштабной трансформации подразделения безопасности, руководством департамента поставлена задача разобраться с ситуацией. Поступательно проведены этапы: анализ текущей ситуации, определение основных проблемных зон, причин возникновения инцидентов, разработка мер по исправлению и их внедрение.

Введение

Сбер – крупнейший банк Северо-Восточной Европы и экосистема России. В структуре Сбера 11 тыс. отделений и 60 тыс. банкоматов. Сбер обслуживает 3 млн корпоративных и 100 млн розничных клиентов, которые совершают 42 млрд транзакций в год.

В структуре Сбера Департамент безопасности отвечает за направления комплексной и экономической безопасности: оценка и мониторинг деловой репутации, бенефициарные связи, проектирование и мониторинг технических средств охраны, реагирование на преступные посягательства, физическая защита объектов банка.

Владелец процесса в Сбере – это самостоятельное структурное подразделение банка, которое является основным методологом, определяющим правила выполнения этого процесса и, чаще всего, основным исполнителем. На начало проекта владелец процесса определял самостоятельно наличие проблемных зон в каждом процессе, меры минимизации и риск стратегию (принятие, снижение, избегание, передача) по ним, в том числе по направлению безопасности.

Отдельные процессы, сценарии процессов и внутренние нормативные документы (далее – ВНД) по направлению Модели угроз безопасности, риска безопасности отсутствовали.

Бизнес-контекст

Анализ ситуации

Сначала проведен анализ внутренней ситуации в подразделении:

- в конце 2021 года Департамент безопасности являлся владельцем 30 процессов основной их контекст реагирование. Реагирование на заявки смежных подразделений, запросы правоохранительных органов, реализованных событий безопасности
- интеграция процессов и функций с системой управления рисками отсутствует
- хранение информации о реализованных событиях безопасности локальное, централизованный анализ причин отсутствует
- отсутствует подход к факторному анализу видов и причин реализованных событий безопасности в рамках операционного риска банка.

Далее проведен анализ ситуации в банке:

- развернута профессиональная система управления рисками, в том числе и операционными в соответствии с действующими требованиями регулятора
- события безопасности учитываются в системе операционных рисков, оцениваются и управляются владельцем процесса, в котором выявлены, в рамках лимита операционного риска подразделения

- атомарная величина события безопасности, характеристики и единые решения по минимизации отсутствуют
- при проектировании нового процесса или внесении изменений в существующий процесс отсутствует экспертиза безопасности
- выявлен рост числа и суммы убытков от реализованных событий по линии безопасности.

Следующий шаг - внешний анализ:

- взаимодействие банков и правоохранительных органов в европейских странах отличается от российской практики, результатом является отсутствие в Базеле II и III отдельного риска безопасности или одноименной внутренней группы операционного риска
- отсутствие требований регулятора к безопасности в рамках риск-стратегий банка
- предыдущие два пункта и чувствительность направления привели к скудному количеству информации по данной теме на рынке в целом и банковской отрасли в частности.

Определение основных проблемных зон

- отсутствие методологии: понятие, взаимосвязи, атрибуты и характеристики
- отсутствие процессов и системной работы по прогнозированию, аналитике, предотвращению
- отсутствие анализа структуры ущерба, системных мер предотвращения и контроля реализации
- отсутствие интеграции профессионального управления рисками (угрозами) безопасности и методологии управления операционными рисками банка.

Разработка мер

Создание Модели угроз

Первым шагом стало создание Модели угроз безопасности. Определили атомарную единицу безопасности в операционном риске – угроза безопасности. См. рис. 1

Угроза безопасности – разновидность операционного риска, единица Модели угроз

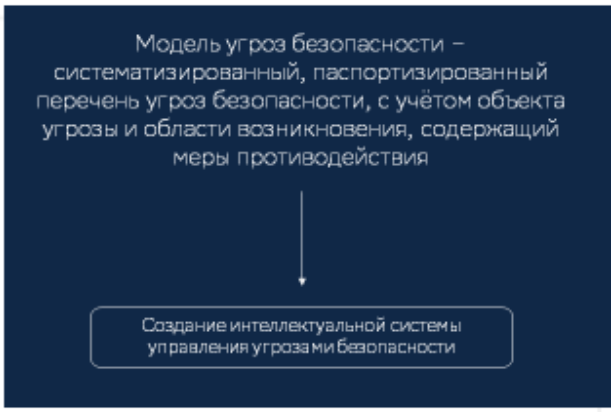


Рис.1

На основании сбора и анализа локальных архивов событий преступных посягательств за последние 10 лет сформировали каркас модели – Матрицу угроз безопасности.

Принцип структуры, а точнее, взаимозависимостей взят из таблицы Пифагора, а тематическими вертикалями и горизонталями стали: объекты угрозы и области возникновения.

Пересечения горизонталей и вертикалей образуют группы угроз безопасности, каждая из которых имеет свой уникальный идентификатор и список угроз безопасности. См. рис. 2

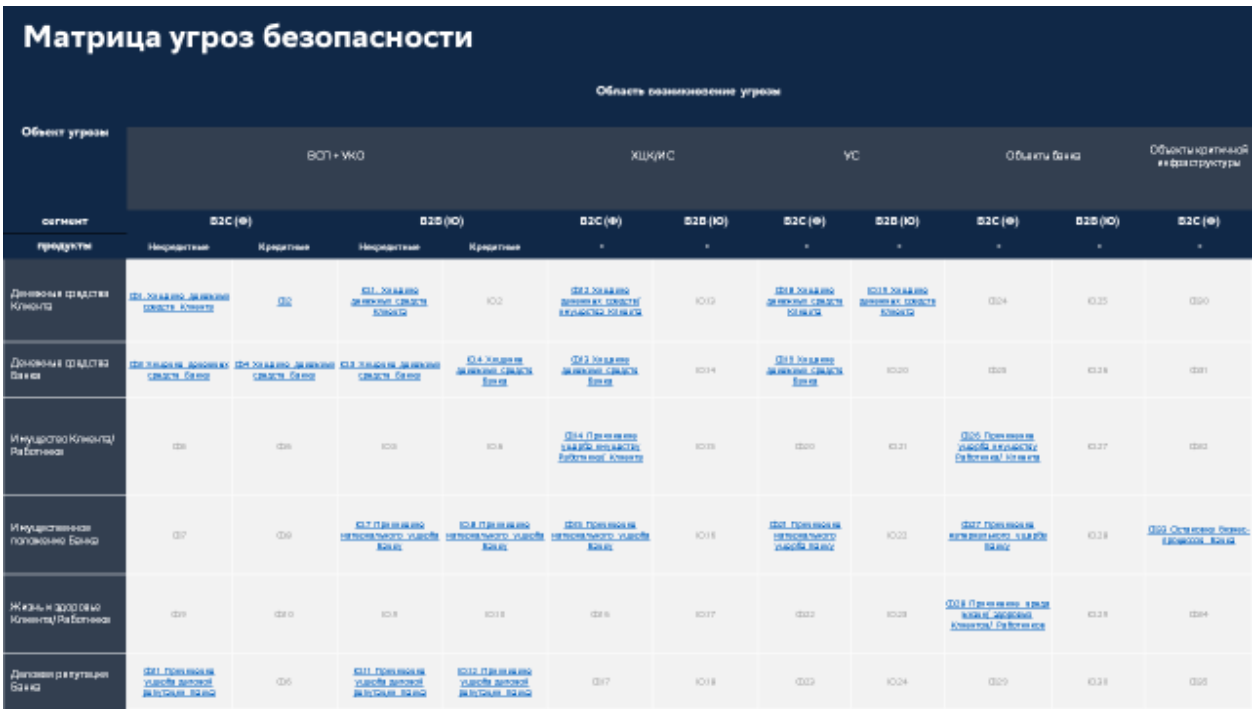
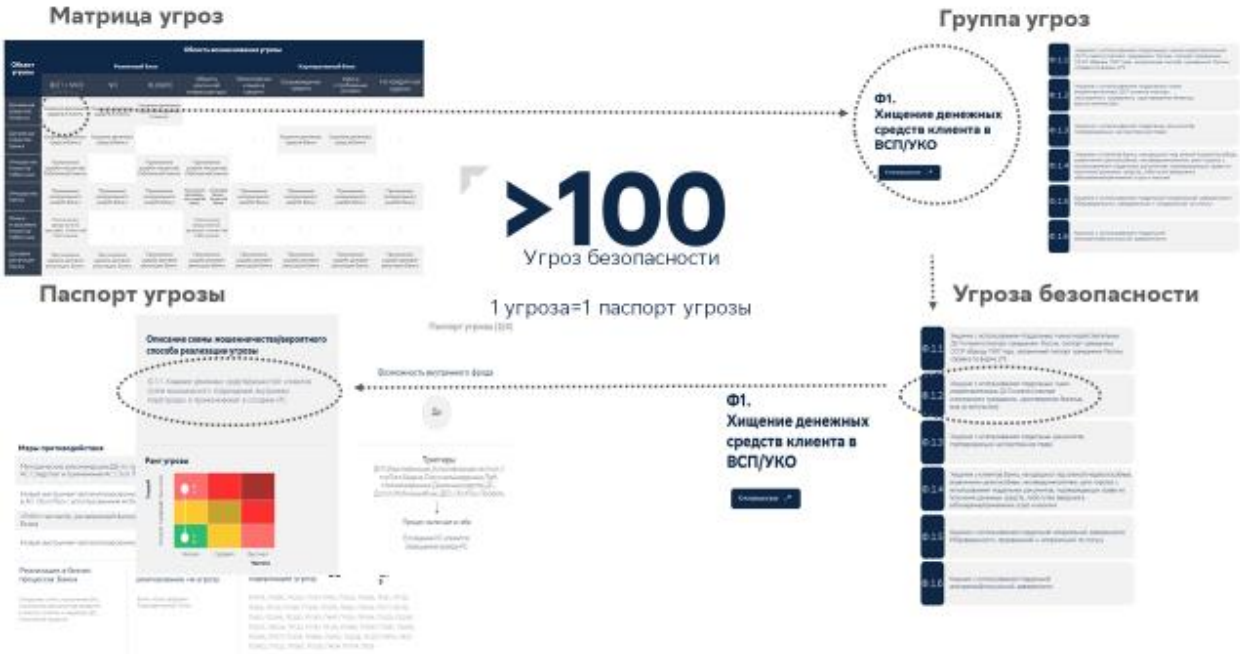


Рис.2

Для каждой угрозы безопасности разработан паспорт угрозы с атрибутами:

- способ реализации/схема мошенничества
- ранг угрозы – расчет вероятности и влияния
- меры противодействия: фронт – процессные и бэк – системные
- наличие или отсутствие возможности внутреннего фрода
- триггеры. См. рис.3



В начале пути определили концепцию, что созданный перечень угроз является фундаментом, который не изменяется под конкретный процесс, а определяется наличием одной или нескольких угроз из актуального перечня в конкретном процессе, проекте или продукте. Изменение Матрицы угроз и перечня угроз проводится по единым правилам, которые будут закреплены в соответствующем процессе.

Процесс завершения формирования Матрицы и перечня угроз совпал с 1 кварталом 2022 года, что внесло корректировки в сроки реализации проекта, его актуальности и списка угроз. Ряд угроз безопасности, которые на начало формирования Модели угроз казались фантастическими и низковероятностными, были актуализированы и приобрели красный оттенок. Все события этого периода подтвердили правильность пути анализа и прогнозирования угроз безопасности как важной составляющей системы управления рисками банка.

Взаимодействие с Рисками

Следующим шагом стало определение роли Департамента безопасности в текущей системе управления операционным риском – профессионального управляющего угрозами безопасности. См. рис. 4

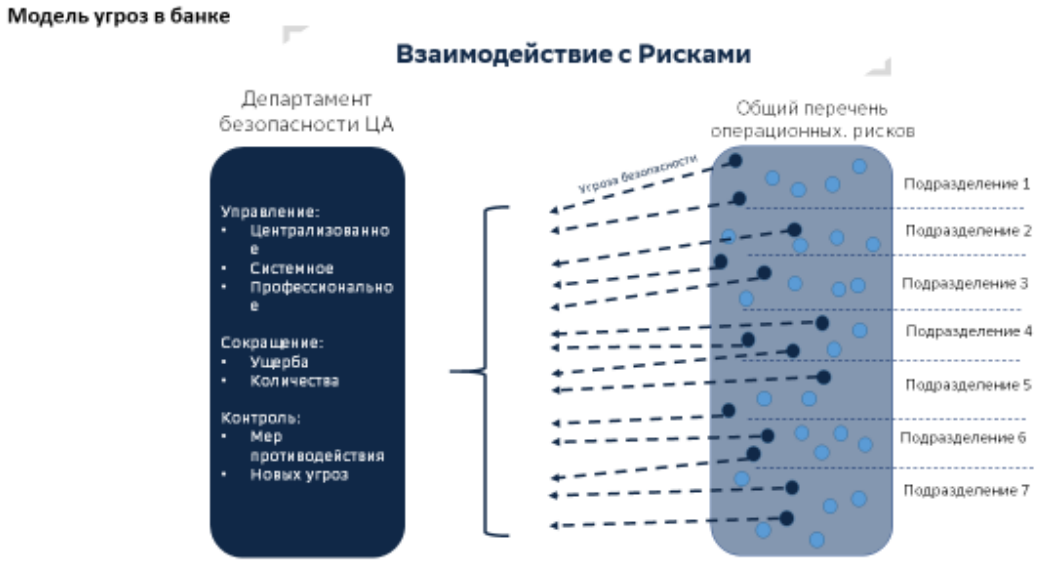


Рис.4

Такое самоопределение является критически важным для выстраивания системной работы:

- определение наличия уязвимостей к угрозам безопасности в банке (идентификация угроз)
- применение мер противодействия
- мониторинг
- фиксирование и консолидация случаев реализации одной угрозы в различных процессах
- определение способов реализации угроз безопасности
- своевременная актуализация Модели угроз безопасности.

Интеграция основных этапов системы управления операционным риском и управления Моделью угроз безопасности сформулирована в пяти шагах цикла управления. См. Рис.5. На следующих этапах развития проекта интеграция реализована в конкретных инструментах.

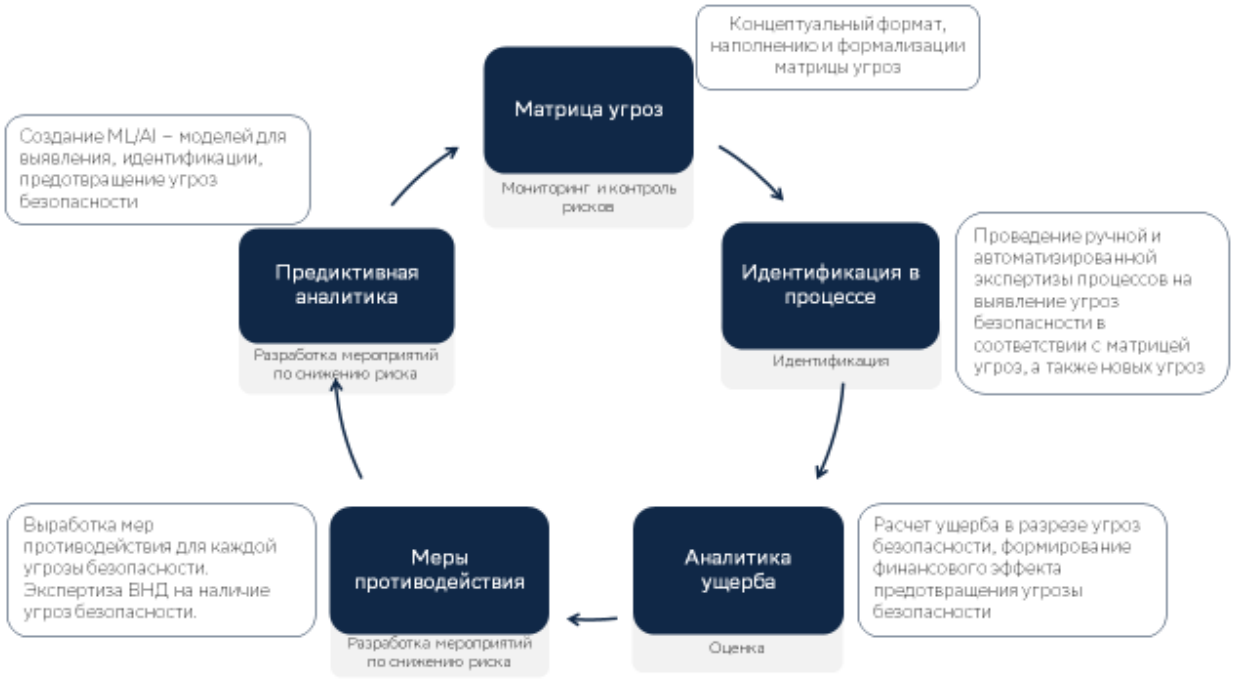


Рис.5

Идентификация

После формирования понимания, что такое угроза безопасности, как она возникает и на сколько она критична для Сбера, необходимо было сформировать подходы определения наличия угроз.

Первым методологическим рубежом стали процессы банка.

Учитывая, что в банке 2300 процессов, которые постоянно изменяются, их объем описательной части достигает 600 страниц, а вложенность сценариев может составлять 5 уровней, разброс тем от эксплуатации до международных филиалов, было необходимо найти унифицированные методы поиска угроз в процессе.

Главный принцип системного рассмотрения процессов – моделирование. При рассмотрении процесса, осознанно отошли от точечного рассмотрения. Необходимо рассмотреть процесс полностью, смоделировав все возможные варианты развития событий.

Инструментами для решения стали:

- алгоритм идентификации
- матрица и перечень угроз (определение от места и обстоятельств, возможных событий)
- чек-лист – дерево решений, состоящее из вопросов ответы на которые формируют возможный перечень угроз для конкретного процесса.

Степень защищенности и ранг угрозы

Каждая угроза имеет ранг, который складывается из вероятности реализации события и влияния – суммы возможного убытка и является условно постоянным: пересчитывается с заданной периодичностью на основании полученных за период данных. Ранг визуализируется цветом тепловой шкалы и соответствующими показателям баллами в формате координат (x, y). См. рис.6

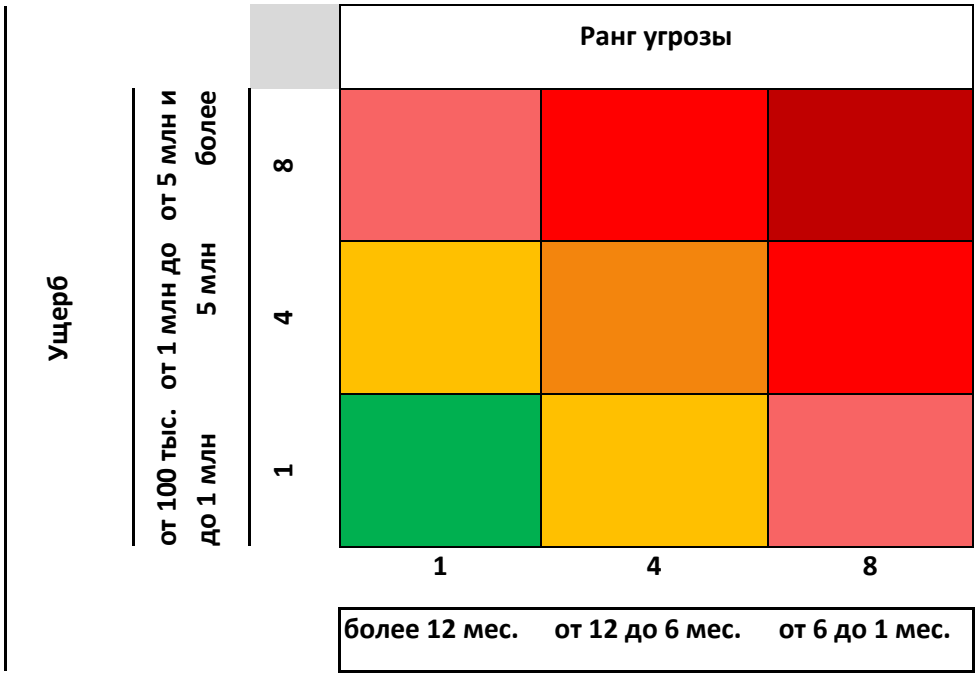


Рис.6

При рассмотрении процесса на наличие угроз безопасности результатом может быть выявление нескольких угроз, расчет сочетания их влияния и вероятности формирует степень защищенности процесса, который контролируется при мониторинге. В сборнике методик по Модели угроз

безопасности подробно описывается расчет данного показателя, так как он является практически применяемым и основополагающим для мониторинга состояния безопасности процессов банка.

Мониторинг

В Модели угроз мониторинг - этап контроля и фиксирования появления отклонений на ранних стадиях для своевременного определения причин и приятия стандартных мер противодействия или выработки новых. Внеплановая выработка новых мер противодействия может потребоваться при определении причин снижения степени защищенности:

- новый способ реализации/схема мошенничества
- новая угроза
- назначенные меры реализованы, но утратили влияние на реализацию.

Все разработанные подходы по порядку идентификации, определения степени защищенности процессов и продуктов, формирование и актуализация мер противодействия, мониторинга угроз безопасности и степени защищенности процессов[1] и продуктов сформировали в сборник методик по Модели угроз безопасности.

Данный сборник направлен регулятору в качестве подтверждения нормативного исполнения новых требований 716-П от 25.03.2022.
В изменениях нормативного документа регулятора появилось требование о модели угроз. Время надиктовало совпадение маршрутов развития банка с требованиями регулятора практически одномоментно.

Процессы

Одновременно с разработкой методологии: описание подходов, правил и методик проектировались процессы.

Процессная структура проекта следующая:

- внутренние этапы работы подразделения безопасности
- этапы взаимодействия с подразделениями банка
- управляющий процесс.

В результате созданы и утверждены процессы:

- Идентификация угроз безопасности в процессах и продуктах банка
- Выявление, оценка и мониторинг событий реализации угроз безопасности
- Актуализация Модели угроз безопасности.

[1] Степень защищенности объектов банка – часть добавлена в Сборник методик в 2023 году.

В 2022 году команда из шести человек на уровне центрального аппарата ПАО Сбербанк завершила методологическую часть разработки Модели угроз безопасности, результатам которой стали:

- создана Модель угроз безопасности с ее атрибутами: матрица, перечень угроз, паспорта с рангами угроз и мерами противодействия. Итоговое количество более 100 угроз безопасности
- разработаны и утверждены четыре методики
- разработаны, утверждены и внедрены три процесса
- интегрированы управление операционными рисками и Моделью угроз безопасности.

Следующий этап внедрения был осложнен тем, что в банке действовали 2300 процессов, а Модель угроз безопасности только сформировалась в первой итерации, поэтому внедрение необходимо было совместить с организацией конвейера основной задачей которого было синхронизировать текущий процессный статус и зрелость Модели угроз.

Бизнес-процессы

В Сбере действуют правила конфиденциальности, которые распространяются на бизнес-описания процессов. Процессы Модели угроз безопасности имеют индекс К-1 (высшая степень конфиденциальности), поэтому здесь будут представлены только верхнеуровневые схемы, без детализации сценариев и описательной части.

Идентификация угроз безопасности в процессах и продуктах Банка

В процессе описаны этапы идентификации и сценарии по стандартной и углубленной идентификации. Этот процесс используется только подразделением центрального аппарата и подразделением на межрегиональном уровне[2]. Рис.7

В описании процесса идет ссылка на соответствующие части и главы сборника методик и форматы документов.

[2] Межрегиональное подразделение было запроектировано заранее и не существовало в момент разработки процесса.

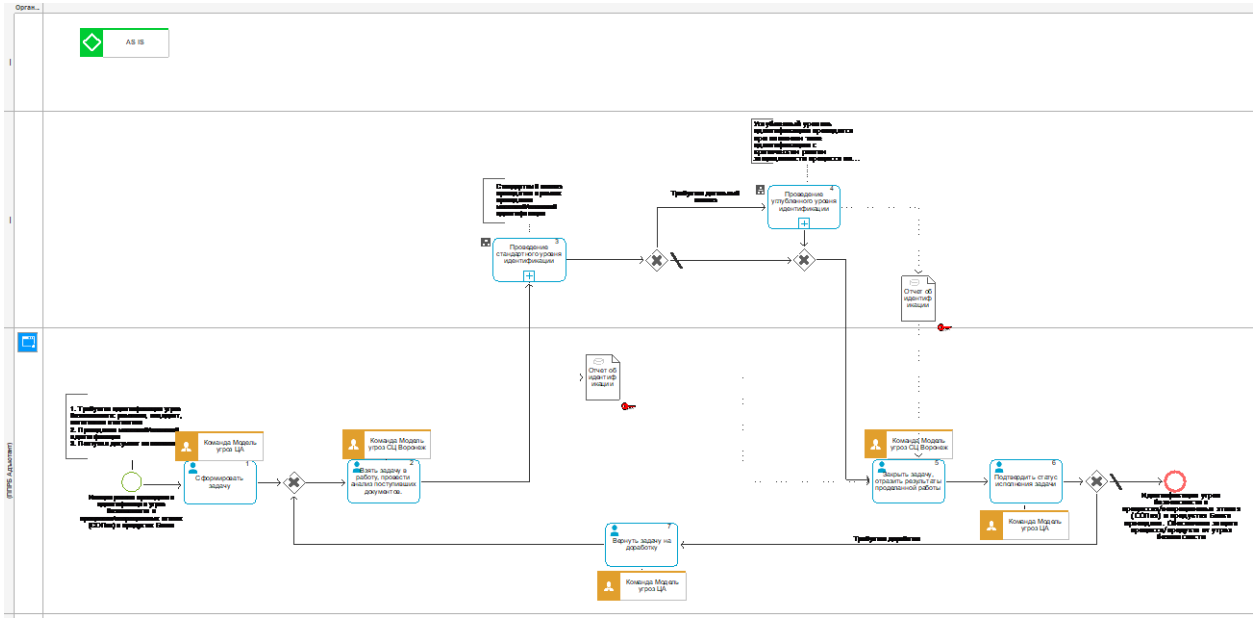


Рис.7

Выявление, оценка и мониторинг событий реализации угроз безопасности

В процессе описаны входящие внешние события, условия и переходы в смежные процессы Модели угроз по идентификации и актуализации угроз безопасности, подготовка, оформление, рассмотрение и арбитраж результатов идентификации в подразделениях банка. Рис.8

Также сценарием процесса является мониторинг с указанием шагов постановки процессов, контроля степени защищенности, оценки эффективности мер противодействия и эскалации при неисполнении мер противодействия.

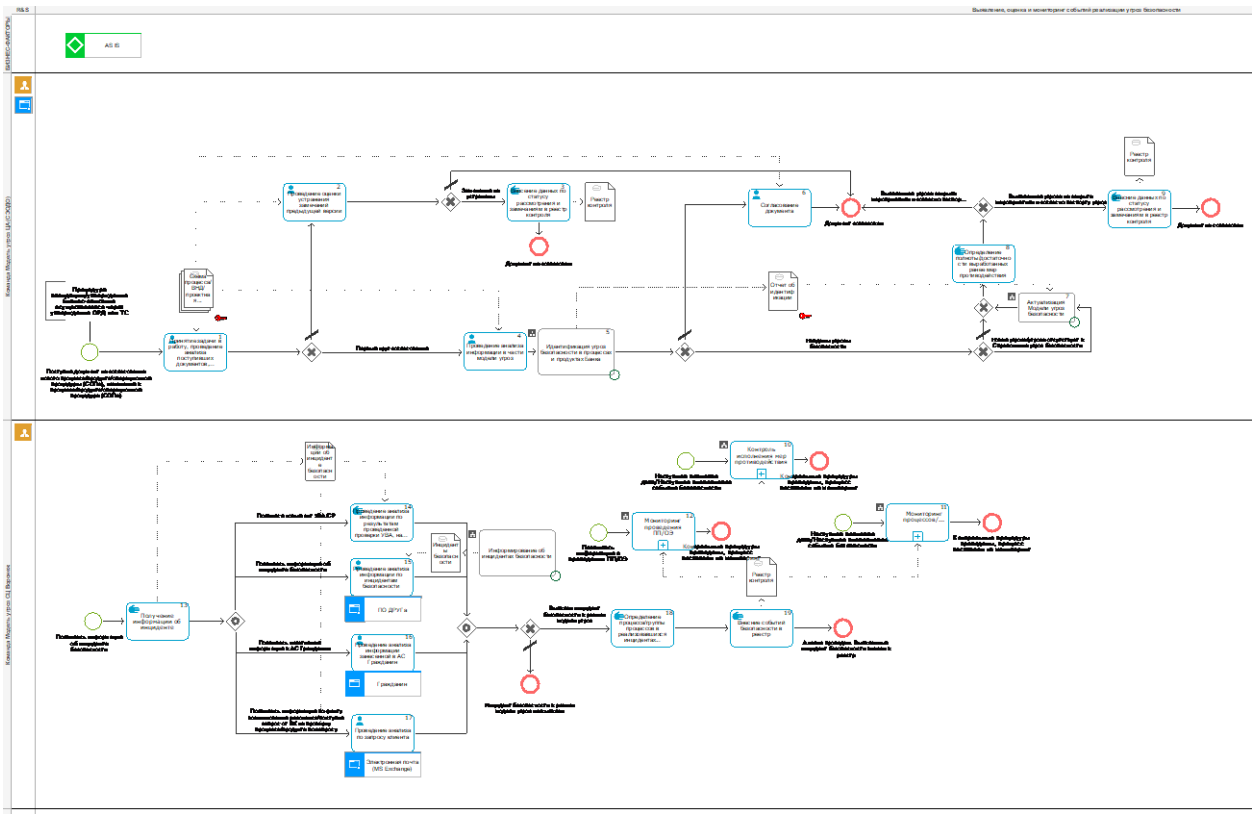


Рис.8

Актуализация Модели угроз безопасности

Управляющий процесс, который описывает порядок, условия и сценарии внесения изменений в Модель угроз:

- архивирование утративших актуальность угроз
- добавление и описание новых угроз
- создание новых паспортов угроз безопасности
- изучение, описание и добавление способов реализации
- разработка и добавление мер противодействия
- взаимодействие с экспертами внутри Департамента безопасности и другими подразделениями банка. Рис.9

Взаимодействие с другими подразделениями банка, важная составляющая работы Модели угроз, так как банк сложный механизм и при моделировании необходимо принимать во внимание факторы из смежных областей: сегмент клиентов, канал обслуживания, продукт, личное присутствие клиентов, комплект документов, расположение офиса, формат обслуживания и т.д.

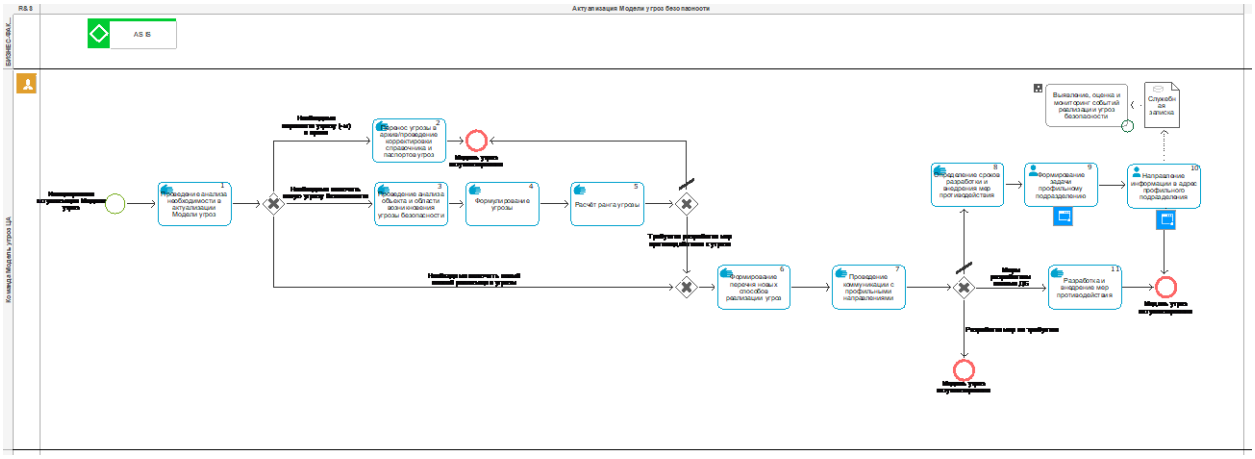


Рис.9

На момент создания данного описания все процессы находятся в стадии редизайна. Необходимо сформировать структуру to be и описать процесс после ввода в промышленную эксплуатацию платформенного решения – автоматизированной системы по контролю и анализу угроз безопасности.

Внедрение

В конце 2022 года принято решение о создании межрегиональной команды Модели угроз безопасности для выполнения run-функций. С Сбере run-функциями являются повторяющиеся действия средней и высокой степени регламентации. Также в Сбере есть два уровня команд:

- территориальные, нахождение и управление соответствующей территориальной единицей банка, предоставление услуг/функций для данной территории
- межрегиональный, нахождение в сервисном центре, управление центральным аппаратом, предоставление услуг/функций для всех/нескольких территорий и/или центрального аппарата.

Функциями межрегиональной команды определены:

- идентификация угроз безопасности в процессах и продуктах банка
- мониторинг угроз безопасности и степени защищенности процессов и продуктов банка
- учет угроз безопасности.

Последовательно выполнены этапы:

- подбор и оформление команды
- обучение сотрудников

- декомпозиция процессов и методик до схем
- формирование схем межтерриториального взаимодействия
- запуск конвейера идентификации и постановки на мониторинг
- разметка исторических данных реализованных инцидентов операционного риска соответствующими угрозами безопасности
- работа в стандартном, отработанном цикле.

При разработке подходов, методик и процессов, которые создавались с «0», команда использовала несколько этапов проработки:

- отрисовка на интерактивной доске (1 этап)
- промежуточное формирование процесса, структуры документа (2 этап)
- проектирование процесса в BPM, оформление документа для рассмотрения (3 этап).

Данный блок по результатам 2023 года:

- функционирует команда из 15 человек
- разработан обучающий курс для новичков
- разработаны схемы взаимодействия. Рабочий пример одного сценария на 2 этапе создания см. рис.10
- разработан новый сценарий идентификации – инцидентный. Рабочий пример на 1 этапе создания См. Рис.11
- запущен конвейер идентификации. См.рис.12
- проведена разметка данных по реализованным с причиной внешнее мошенничество инцидентам операционного риска с 2020 года
- проведен и тиражирован пилотный проект по разметке реализованных с причиной внешнее мошенничество инцидентов операционного риска угрозами безопасности в системе рисков банка. Данный атрибут стал обязательным при классификации событий операционного риска
- работа цикла налажена[3].

[3] Развитие продолжается. В 2024 году на базе команды сформирована лаборатория безопасности для интеграции подходов Модели угроз безопасности с внутренних объектов (процессов и продуктов) на физические объекты (объекты недвижимости, технические системы безопасности и банкоматы).

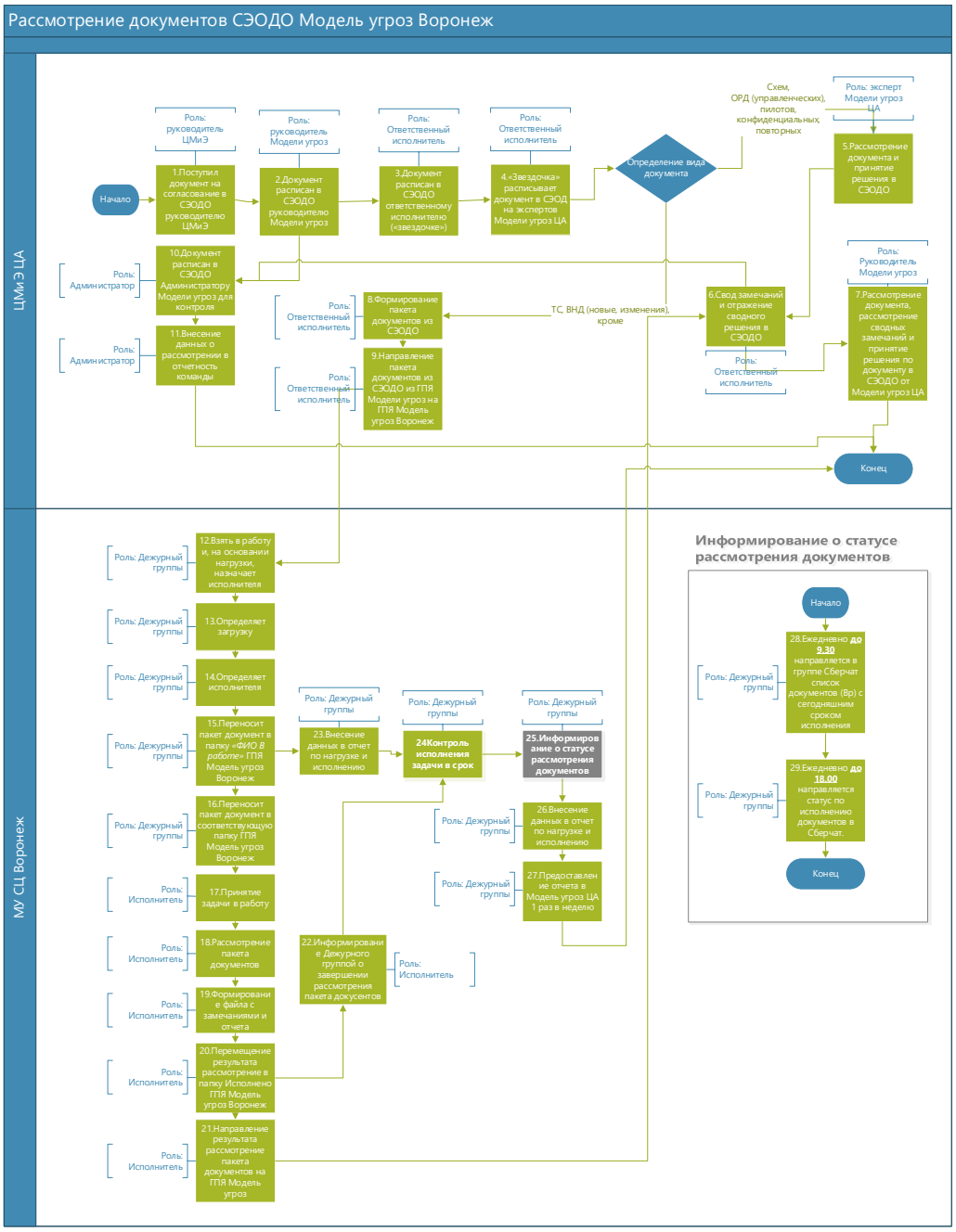

Рассмотрение документов СЭОДО Модель угроз Воронеж
ЦМиЭ ЦА
Начало
Роль: руководитель ЦМиЭ
1.Поступил документ на согласование в СЭОДО руководителю ЦМиЭ
Роль: руководитель Модели угроз
2.Документ расписан в СЭОДО руководителю Модели угроз
Роль: Ответственный исполнитель
3.Документ расписан в СЭОДО ответственному исполнителю («звездочке»)
Роль: Ответственный исполнитель
4.«Звездочка» расписывает документ в СЭОД на экспертов Модели угроз ЦА
Определение вида документа
Схем, ОРД (управленческих), пилотов, конфиденциальных, повторных
Роль: эксперт Модели угроз ЦА
5.Рассмотрение документа и принятие решения в СЭОДО
Роль: Администратор
10.Документ расписан в СЭОДО Администратору Модели угроз для контроля
Роль: Администратор
11.Внесение данных о рассмотрении в отчетность команды
Роль: Ответственный исполнитель
8.Формирование пакета документов из СЭОДО
Роль: Ответственный исполнитель
9.Направление пакета документов из СЭОДО из ГПЯ Модели угроз на ГПЯ Модель угроз Воронеж
ТС, ВНД (новые, изменения), кроме
6.Свод замечаний и отражение сводного решения в СЭОДО
Роль: Ответственный исполнитель
Роль: Руководитель Модели угроз
7.Рассмотрение документа, рассмотрение сводных замечаний и принятие решения по документу в СЭОДО от Модели угроз ЦА
Конец
МУ СЦ Воронеж
Роль: Дежурный группы
12.Взять в работу и, на основании нагрузки, назначает исполнителя
Роль: Дежурный группы
13.Определяет загрузку
Роль: Дежурный группы
14.Определяет исполнителя
Роль: Дежурный группы
15.Переносит пакет документ в папку «ФИО В работе» ГПЯ Модель угроз Воронеж
Роль: Дежурный группы
16.Переносит пакет документ в соответствующую папку ГПЯ Модель угроз Воронеж
Роль: Исполнитель
17.Принятие задачи в работу
Роль: Исполнитель
18.Рассмотрение пакета документов
Роль: Исполнитель
19.Формирование файла с замечаниями и отчета
Роль: Исполнитель
20.Перемещение результата рассмотрение в папку Исполнено ГПЯ Модель угроз Воронеж
Роль: Исполнитель
21.Направление результата рассмотрение пакета документов на ГПЯ Модель угроз
Роль: Дежурный группы
23.Внесение данных в отчет по нагрузке и исполнению
Роль: Дежурный группы
24Контроль исполнения задачи в срок
Роль: Дежурный группы
25.Информирование о статусе рассмотрения документов
Роль: Дежурный группы
26.Внесение данных в отчет по нагрузке и исполнению
Роль: Дежурный группы
27.Предоставление отчета в Модель угроз ЦА 1 раз в неделю
22.Информирование Дежурного группой о завершении рассмотрения пакета докусентов
Роль: Исполнитель
Информирование о статусе рассмотрения документов
Начало
Роль: Дежурный группы
28.Ежедневно до 9.30 направляется в группе Сберчат список документов (Вр) с сегодняшним сроком исполнения
Роль: Дежурный группы
29.Ежедневно до 18.00 направляется статус по исполнению документов в Сберчат.
Конец

Рис.10

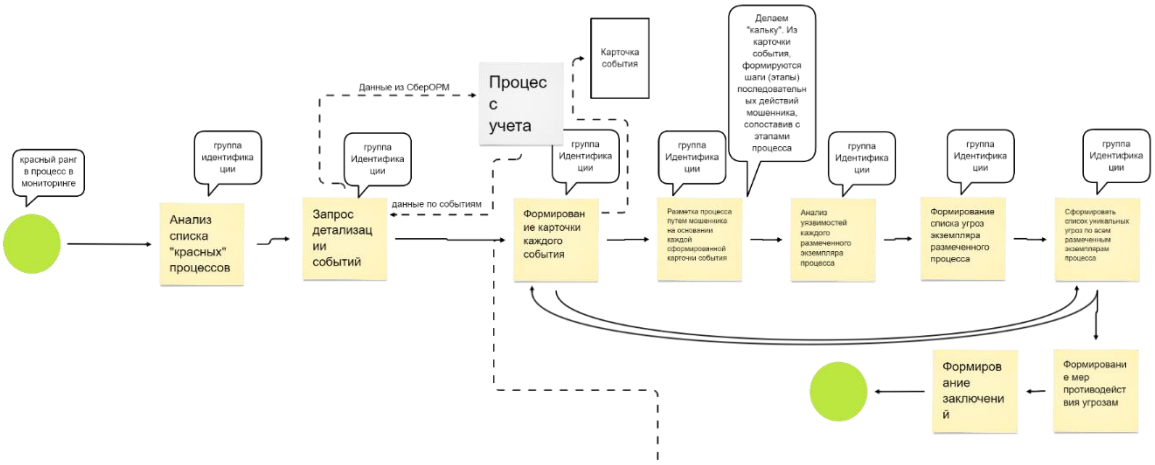

красный ранг в процесс в мониторинге
группа идентификации
Анализ списка "красных" процессов
группа Идентификации
Запрос детализации событий
Данные из СберОРМ
Процесс учета
Карточка события
данные по событиям
группа Идентификации
Формирование карточки каждого события
группа Идентификации
Разметка процесса путем мошенника на основании каждой сформированной карточки события
Делаем "кальку". Из карточки события, формируются шаги (этапы) последовательных действий мошенника, сопоставив с этапами процесса
группа Идентификации
Анализ уязвимостей каждого размеченного экземпляра процесса
группа Идентификации
Формирование списка угроз экземпляра размеченного процесса
группа Идентификации
Сформировать список уникальных угроз по всем размеченным экземплярам процесса
Формирование мер противодействия угрозам
Формирование заключений

Рис.11

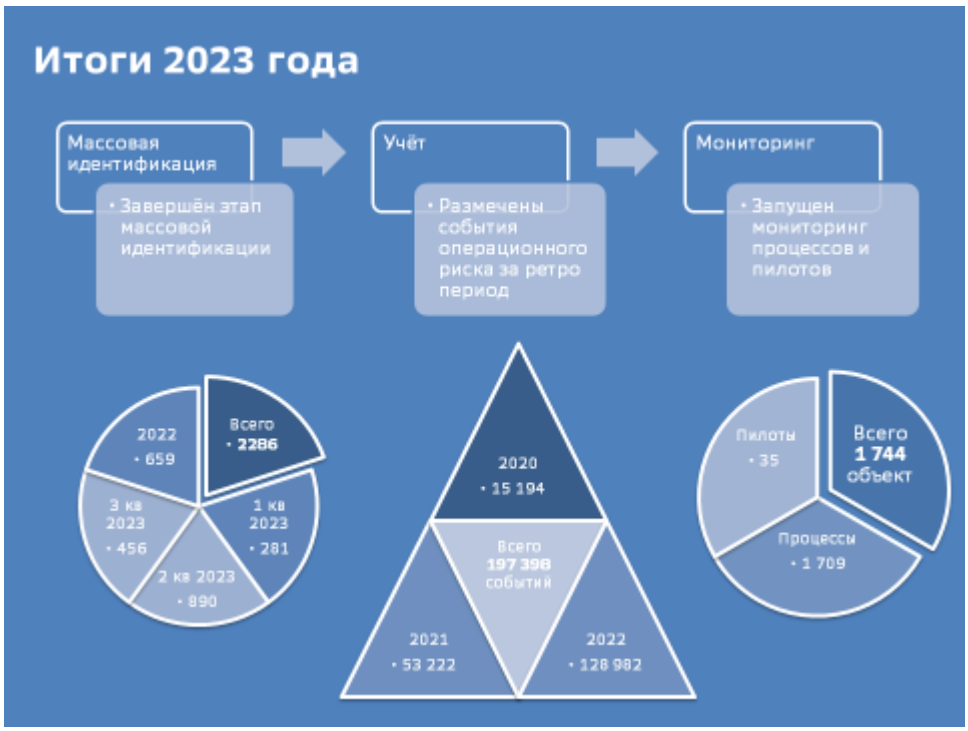


Рис.12

Результаты

- 0 руб. ущерба в 2023 году от преступных посягательств на отделения и банкоматы банка. С учетом Модели угроз поменяли подходы к оснащению объектов банка техническими средствами охраны и укрепленности, приоритизировали, сначала отделения с высоким уровнем угроз безопасности и сформировали адресный подход к усилению инфраструктуры
- 20% потенциально предотвращенный ущерб банка от суммы убытка прошлого периода
- 100% процессов банка идентифицированы на угрозы безопасности
- 100% процессов банка поставлены на мониторинг
- 100% ключевых событий проходят экспертизу Модели угроз безопасности
- создан платформенный продукт – автоматизированная система контроля и анализа угроз безопасности.

Инновационость

Аналогичного системного аналитического продукта безопасности нет на рынке.
Проект продолжает развиваться и поставлены следующие амбициозные задачи, над которыми работает команда:

- синхронизация внутренних объектов (процессов и продуктов) и физических объектов (объекты недвижимости всех категорий, технических средств безопасности, банкоматов)
- проектирование решений, принимаемых подразделением безопасности с учетом Модели угроз безопасности
- прогнозирование реализации угроз безопасности на объектах банка на основании многокритериальной модели, связанной с Моделью угроз безопасности банка.