Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

Кафедра комплексной информационной безопасности электронно-
вычислительных систем (КИБЭВС)

Конев Антон Александрович

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Методические указания к практическим занятиям
и самостоятельной работе студентов

Томск, 2018

Практическая работа №1

Построение модели объекта защиты

Цель работы – получить навыки комплексного построения модели объекта защиты в виде формального описания процесса, связанного с обработкой защищаемой информации.

Задачи:

1. Построение модели «чёрного ящика» данного процесса в нотации IDEF0.
2. Декомпозиция модели на три-четыре этапа в нотации IDEF0.
3. Корректировка модели «чёрного ящика» после декомпозиции на основе уточнённых данных.

Ответ на задание необходимо предоставить в виде файла в формате Word или PDF. В файле должны быть представлены основные результаты работы – модель «чёрного ящика» процесса и её декомпозиция, выполненные в нотации IDEF0.

Критерии оценки:

1. Выполнение задач на базовом уровне (в целом соблюдаются правила нотации IDEF0, этапы декомпозиции соответствуют выбранному варианту) оценивается в **20 баллов**.
2. Выполнение задач на продвинутом уровне (соблюдаются правила нотации IDEF0, этапы декомпозиции и элементы (т.е. стрелки), соответствуют выбранному варианту) и соблюдаются сроки сдачи работы оценивается в **30 баллов**.

Итого за выполнение лабораторной работы можно получить 30 баллов.

Самостоятельная работа заключается в выборе индивидуального варианта информационного процесса, в котором происходит обработка защищаемой информации, и его реализации на основе методики выполнения практического задания.

Варианты процессов

1. Онлайн-оплата покупки банковской картой
2. Получение посылки на почте
3. Отправка конфиденциального электронного сообщения
4. Контроль доступа с помощью СКУД
5. Онлайн-заказ банковской карты
6. Запись на прием к врачу через портал Госуслуги
7. Оформление кредита в банке
8. Запись конфиденциального файла на носитель
9. Снятие наличных через банкомат
10. Покупка электронного билета на самолёт
11. Покупка криптовалюты
12. Установка соединения в Wi-Fi сети
13. Онлайн-заказ такси
14. Онлайн-подача заявления на поступление в ВУЗ
15. Регистрация в социальной сети
16. Онлайн-оплата штрафа за нарушение ПДД
17. Смена паспорта
18. Проведение конфиденциальной видеоконференции
19. Выдача займа в ломбарде
20. Удалённое управление персональным компьютером

Основные принципы функционального моделирования (IDEF0)

IDEF0 – методология функционального моделирования (англ. function modeling) и графическая нотация, предназначенная для формализации и описания бизнес-процессов.

1. Функциональный блок графически изображается в виде прямоугольника и олицетворяет собой некоторую конкретную функцию (действие) в рамках рассматриваемого процесса. Стрелки обозначают объекты различных типов

2. Верхняя сторона блока имеет значение «Управление» и входящие сверху в блок стрелки являются законодательными актами, регламентами, инструкциями, алгоритмами, фиксированными параметрами системы и др.

3. Левая сторона имеет значение «Вход», а правая сторона имеет значение «Выход» и все горизонтальные стрелки являются информацией (или носителем информации) в какой-либо форме представления – документы, файлы и базы данных, сетевые пакеты, количество ресурсов, сумма денег и т.п.

4. Нижняя сторона имеет значение «Механизм» (Mechanism) и входящие снизу в блок стрелки являются исполнителями – сотрудники организации, клиенты, автоматизированные системы, СУБД и т.п.

Более подробную информацию о данной нотации можно получить в рекомендациях Р 50.1.028-2001 "Информационные технологии поддержки жизненного цикла продукции. Методология функционального моделирования".

Пример модели процесса

Тема **– Оплата покупки через контактный банковский терминал**.

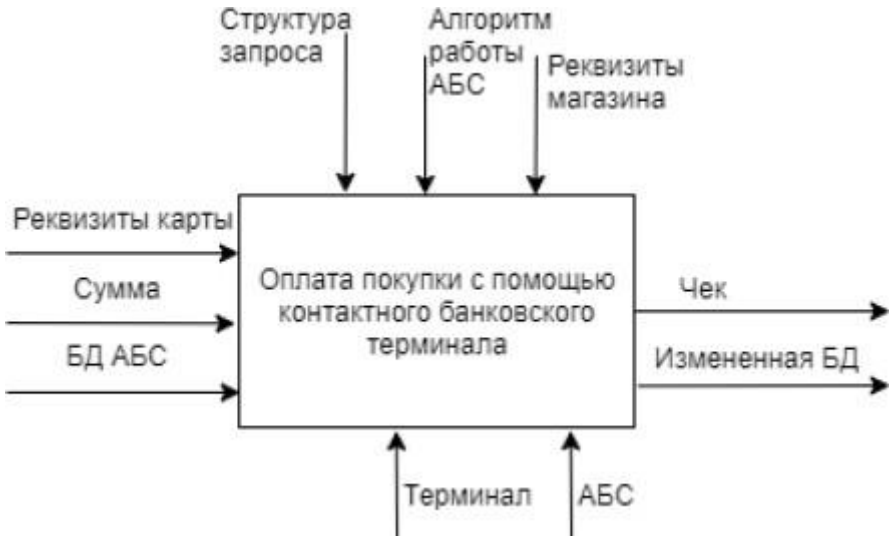

Рисунок 1.1 – Модель «чёрного ящика» процесса в нотации IDEF0

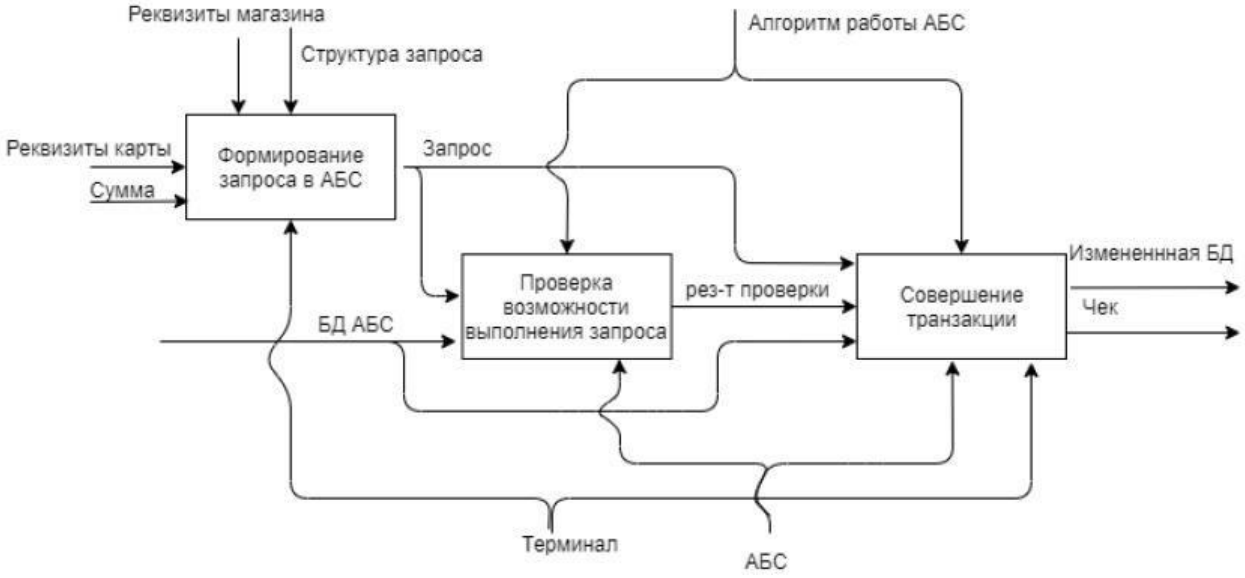

Рисунок 1.2 – Декомпозиция процесса в нотации IDEF0

Практическая работа №2

Моделирование угроз информационной безопасности

Цель работы – получить навыки комплексного моделирования угроз, учитывающего угрозы, направленные на информационную систему и обрабатываемую ей информацию.

Задачи:

1. На основе декомпозиции модели процесса, обрабатывающего защищаемую информацию, выделить перечень защищаемых элементов (все стрелки в декомпозиции) и классифицировать их на три типа – информационные элементы, исполнители, управление.
2. Привести по одному примеру угроз конфиденциальности, целостности и доступности для каждого информационного элемента (горизонтальных стрелок) декомпозиции.
3. Привести по одному примеру угроз конфиденциальности и целостности для каждого механизма реализации процесса (стрелок снизу).
4. Привести по одному примеру угроз конфиденциальности и целостности для каждого элемента управления процессом (стрелок сверху).

Ответ на задание необходимо предоставить в виде файла в формате Word или PDF. В файле должны быть представлены примеры угроз, направленных на различные элементы рассматриваемого процесса.

Критерии оценки:

1. Выполнение задач на базовом уровне (не менее 50% угроз для каждого типа элементов указаны корректно) оценивается в **15 баллов**.
2. Выполнение задач на продвинутом уровне (не менее 80% угроз для каждого типа элементов указаны корректно) оценивается в **20 баллов**.

Итого за выполнение лабораторной работы можно получить 20 баллов.

Самостоятельная работа заключается в реализации индивидуального варианта, выбранного в рамках работы по построению модели объекта защиты, на основе методики выполнения практического задания.

Примеры угроз для различных типов стрелок.

Все → (горизонтальные стрелки) – это *информация* либо *носители информации*. Примеры угроз, направленных на информационные элементы: разглашение или перехват информации ограниченного доступа; несанкционированный доступ к документам; подделка документов; дезинформация; блокирование информации и т.п.

Все ↑ (вертикальные стрелки снизу) – это *исполнители*. Примеры угроз, направленных на автоматизированные системы и людские ресурсы: несанкционированное отключение системы или её модуля; сбор информации о системе (её местонахождение, настройки и др.); повышение привилегий за счёт входа под чужой учётной записью; шантаж или подкуп сотрудника и т.п.

Все ↓ (вертикальные стрелки сверху) – это *управление*. Примеры угроз, направленных на управляющие, регламентирующие и нормативные данные, которыми руководствуются исполнители: внесение недекларированных возможностей в программное обеспечение; разработка нормативных документов, не соответствующих законодательству; нарушение правил работы с конфиденциальной информацией и т.п.

Пример моделирования угроз

Тема **– Оплата покупки через контактный банковский терминал**.

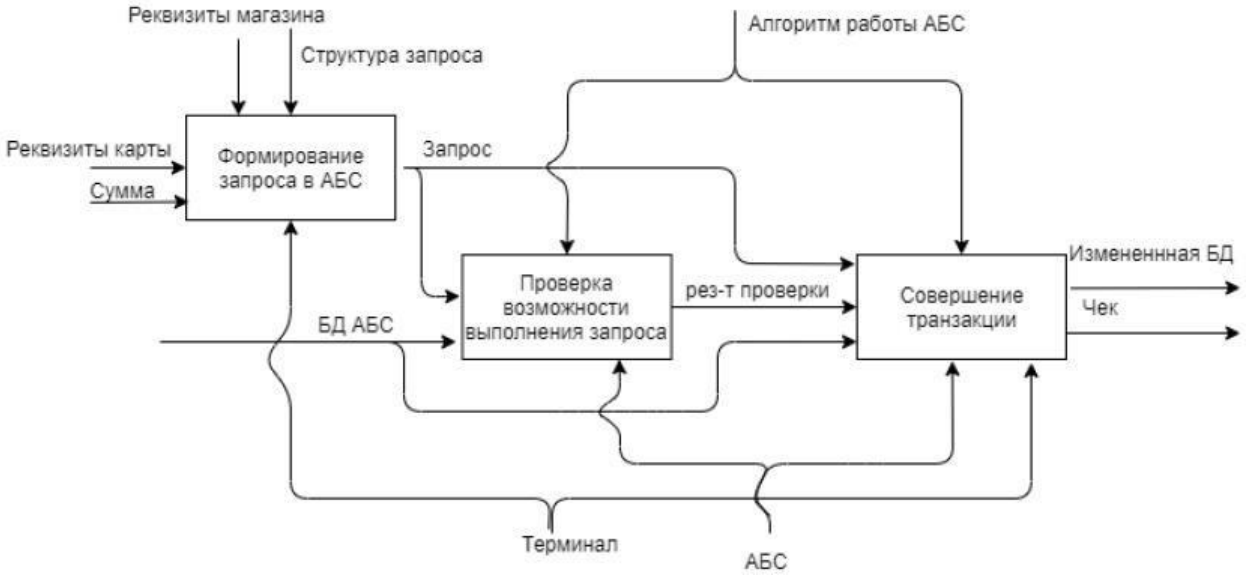

Рисунок 2.1 – Декомпозиция процесса в нотации IDEF0

Таблица 2.1 – Перечень угроз

Тип элемента	Наименование элемента	Угрозы, направленные на элемент		
		Конфиденциальности	Целостности	Доступности
→	База данных автоматизированной банковской системы (БД АБС)	Несанкционированный доступ к базе данных	Несанкционированное уничтожение данных в БД	Блокирование информации из-за перегрузки сетевого канала передачи данных
	Реквизиты карты	Утечка видовой информации	Некорректное считывание реквизитов терминалом	Блокирование информации из-за неработоспособности банковской карты
	Сумма	Общедоступная информация	Некорректный ввод данных	Блокирование информации из-за неработоспособности терминала
	Запрос	Перехват сетевых пакетов, содержащих запрос	Несанкционированное изменение содержимого сетевых пакетов	Блокирование информации из-за перегрузки сетевого канала передачи данных
	Результат проверки	Общедоступная информация	Выдача некорректного результата проверки	Блокирование информации из-за перегрузки сервера с АБС
	Чек	Печать в чеке реквизитов карты	Выдача некорректной информации о банковской транзакции	Блокирование информации из-за неработоспособности терминала
	Изменённая БД	Несанкционированное копирование базы данных на съёмный носитель	Несанкционированное изменение данных в БД	Блокирование информации из-за неработоспособности драйвера базы данных
↑	Терминал	Сбор злоумышленником информации о модели	Несанкционированное отключение терминала	–

		терминала, встроенной операционной системе и т.п.		
	АБС	Сбор злоумышленником информации о версии АБС, открытых портах и т.п.	Заражение АБС вирусом	–
↓	Структура запроса	Разглашение структуры запроса разработчиками	Ошибки на этапе разработки	–
	Алгоритм работы АБС	Получение злоумышленником алгоритма работы АБС при помощи дизассемблирования	Внесение недекларированных возможностей на этапе разработки	–
	Реквизиты магазина	Общедоступная информация	Несанкционированное изменение на этапе внесения данных	–