# Введение

В последние десятилетия мы наблюдаем возрастающее количество киберугроз и угроз конфиденциальности данных. С развитием технологий и цифровизации многие аспекты нашей жизни стали зависеть от информационных систем и передачи данных через интернет. Поэтому сегодня остро стоит вопрос информационной безопасности.

В этом контексте разработка программного обеспечения, помогающего созданию мер защиты, становится одним из приоритетов.

Целью данной работы является создание программного обеспечения, предназначенного для разработки схем информационных потоков в телекоммуникационных системах. В контексте постоянно меняющейся угрозовой среды и появления новых видов атак, особенно важно своевременное развитие документации, регулирующей меры информационной защиты.

Объект исследования: разработка схем информационных потоков.

Предмет исследования: программное обеспечения для разработки схем информационных потоков.

В ходе работы будет проведен анализ инструментов, разработан собственный программный продукт. Это позволит не только повысить уровень защиты информационных систем, но и обеспечить более эффективное использование человеческого ресурса в процессе защиты информационных систем.

Сегодня мы живем в цифровом веке. Поэтому почти все компании уделяют особое внимание информационной безопасности для защиты информации своей или своих клиентов. Начнем с определений. Информация – это любые сведения, или цифровые данные, или сообщения, или документы, или файлы, которые могут быть переданы получателю информации от источника информации.

Информационная безопасность (ИБ) — состояние защищенности информации от внутренних и внешних угроз, способных нанести ущерб интересам личности, общества, государства (национальным интересам). Предметной областью информационной безопасности являются:

* информация и ее свойства;
* угрозы безопасности информации и ее собственникам;
* политика безопасности и модели безопасности;
* защита информации (обеспечение целостности, конфиденциальности и доступности информации, передаваемой или хранимой в какой-либо форме);
* классификация систем защиты;
* требования к защищенности информационных систем (систем, организующих обработку информации о предметной области и ее хранение);
* методология оценки защищенности информационных систем и проектирования защиты.
* конкретные системы защиты информации, применяемые в различных органах управления, учреждениях и на предприятиях различных форм собственности.

Все эти понятия должны быть описаны в соответствующей документации: политики и планы. Политика ИБ — совокупность документированных методологий и управленческих решений, а также распределение ролей и ответственности, направленных на защиту информации, информационных систем и ассоциированных с ними ресурсов. План ИБ – документ, определяющий обязанности и ожидаемое поведение всех людей, имеющих доступ к системе, а также меры безопасности (выбранные или планируемые).

# Анализ состояние проблемы

В настоящее время разработкой занимаются специалисты по информационной безопасности вручную с помощью DrawIO. Это увеличивает время разработки документации, а как следствие – увеличение сроков сдачи проекта. Данная работа предлагает решение для разработки схем информационных потоков из таблиц взаимодействия (и наоборот).

# Основная часть

Для разработки документов необходим сбор исходных данных. Эти данные содержат несколько разделов, среди которых представлены набор оборудования и его взаимодействия. Для отражения взаимодействия компонентов системы разрабатывают таблицы взаимодействия и схему информационных потоков в рамках модели OSI.

OSI (Open Systems Interconnection) – открытая модель сетевого взаимодействия, она состоит из 7 уровней:

1. Приложения - обеспечивает взаимодействие приложений, используемых для коммуникации, и базовой сети, по которой передаются сообщения.
2. Представления - использует протоколы, позволяющие конвертировать и преобразовывать данные.
3. Сеансовый - содержит протоколы, которые управляют сеансом передачи данных.
4. Транспортный – уровень управления передачей данных.
5. Сетевой - предназначается для определения пути передачи данных.
6. Канальный – протоколы, которые используются для разбора потока нулей и единиц и деления этой последовательности бит на блоки данных.
7. Физический - среда, по которой передаются данные

Систему представляют в двух схемах/таблицах взаимодействия информационных потоков: физической и логической. Физическая – отражает одноименный уровень модели, а также указывает на физическое соединение двух компонентов системы («штекер в штекер»). Логическая – отражает транспортный уровень: взаимодействие компонентов с точки зрения конечного обмена информации (минуя промежуточные) с указанием протоколов обмена информации и их назначением.

Программное обеспечение менеджмента связей программно-технических средств информационных систем на основе ядра геометрического моделирования представляет из себя desktop приложение, позволяющее на основании компонентов системы и их связей, занесенных в таблицы базы данных, спроектировать физические и логические схемы информационных потоков с указанием протоколов связи и характеристик компонентов.

///

Информация о кружках-треугольниках и о проделанный работе. Также можно написать о выбранных инструментах разработки с обоснованием.

///

# Список литературы

1. “Защита информации”, Учебное пособие, Габидулин Эрнст Мухамедович, Кшевецкий Александр Сергеевич, Колыбельников Александр Иванович, Владимиров Сергей Михайлович
2. «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ», Е. В. ВОСТРЕЦОВА
3. «Руководство по разработке планов обеспечения безопасности для федеральных информационных систем», Marianne Swanson, Joan Hash, Pauline Bowen
4. Компьютерные сети, М. М. Климанов
5. ISO/IEC 2382:2015