КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ УГРОЗ

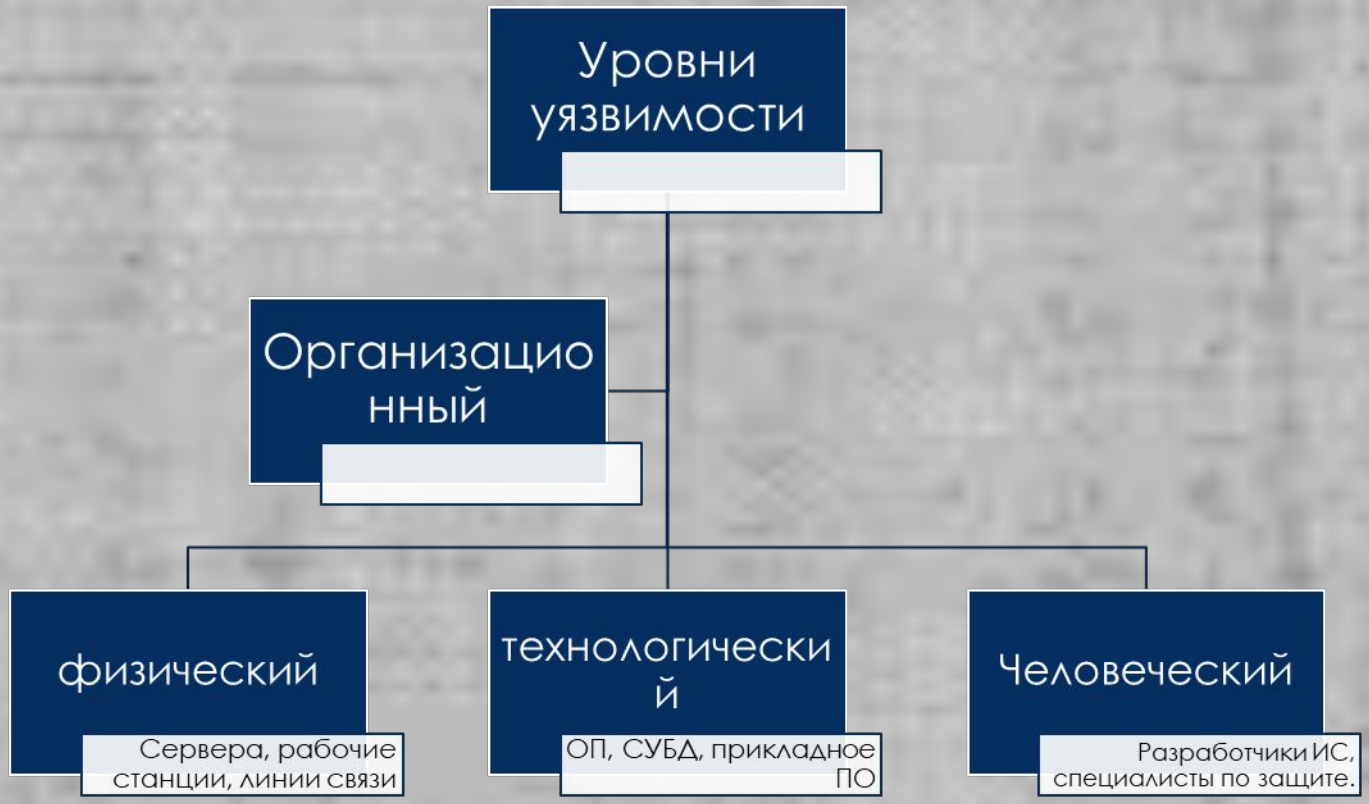
Трухин Денис Александрович 1 курс
17 группа

2020 год

ТаблицаТаблица, иерархияТаблица, иерархия, диаграммаТаблица, иерархия, диаграмма, блок схема

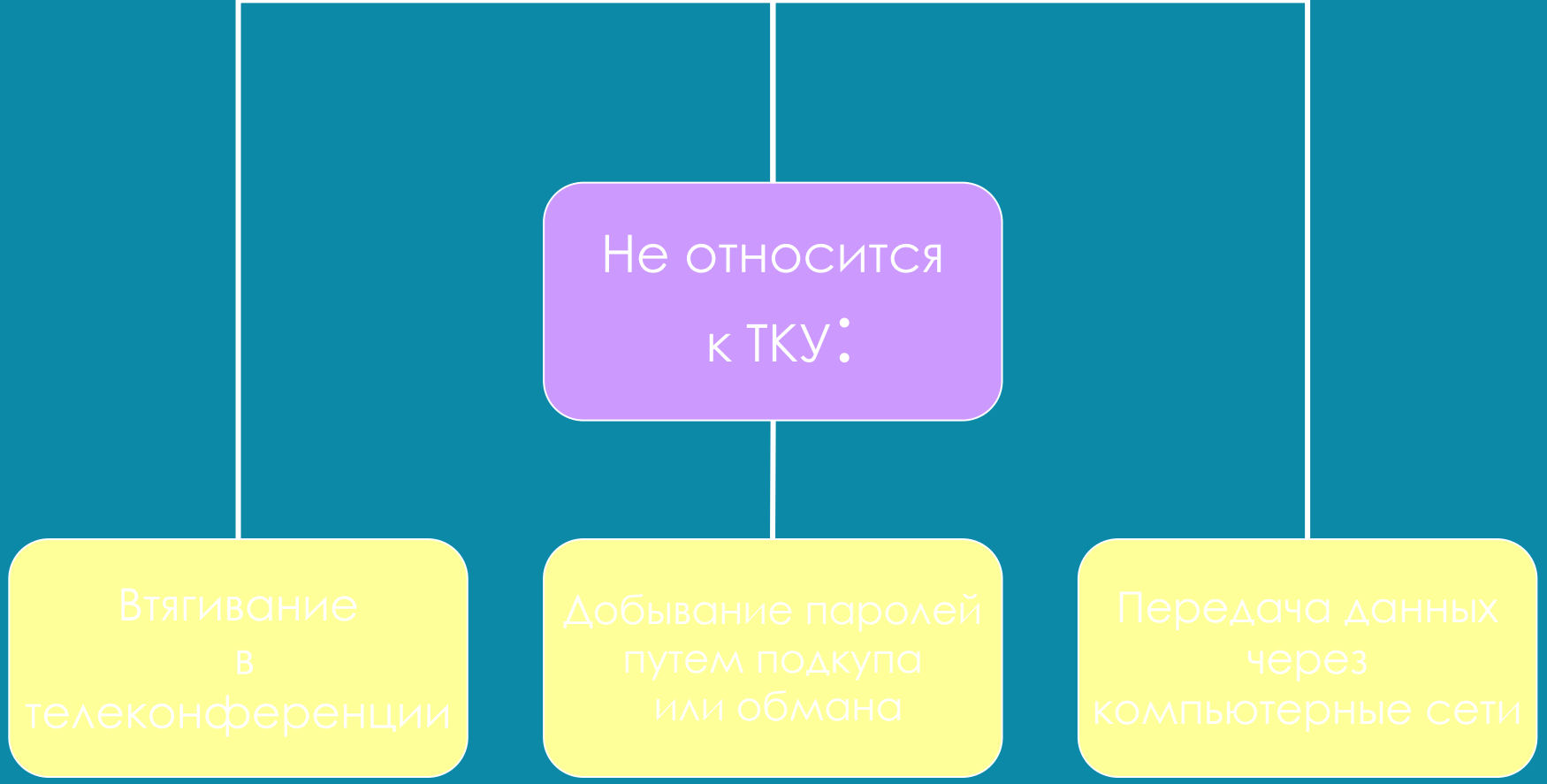
ОБЩЕЕ ПОНЯТИЕ О ТКУ

- Объектом защиты информационной безопасности от технических компьютерных угроз (ТКУ) являются компьютерные системы и сети. Путем реализации ТКУ можно также получать данные непосредственно о пользователях (людях и программах) компьютерных систем и сетей, о режимах их работы, об их интересах и т.п.
- Таким образом, ТКУ - добывание информации из компьютерных систем и сетей, характеристик их программно-аппаратных средств и пользователей.



УРОВНИ УЯЗВИМОСТИ

ТИТУЛЬНЫЙ



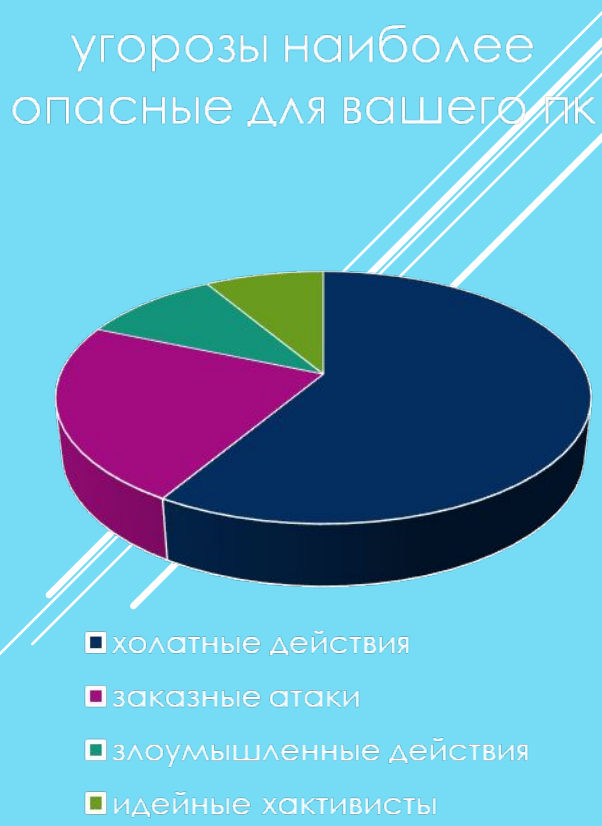
Т. К. СЕТЬ В ДАННОМ СЛУЧАЕ ВЫСТУПАЕТ НЕ БОЛЕЕ ЧЕМ КАК КАНАЛ СВЯЗИ.

ТИПЫ ИНФОРМАЦИИ ДЛЯ ТКУ

Выделим 3 типа источников информации для ТКУ:

- Данные, сведения и информация обрабатываемые, передаваемые и хранимые в компьютерных системах и сетях
- Характеристики программных, аппаратных и программно-аппаратных комплексов
- Характеристики пользователей компьютерных систем и сетей

ДИАГРАММА С НАИБОЛЕЕ ОПАСНЫМИ УГРОЗАМИ



Титульный

КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ УГРОЗ

ИДЕНТИФИКАЦИЯ ОПАСНОСТИ

ТИТУЛЬНЫЙ

- - добывание данных путем использования заранее внедренных изготовителем программно-аппаратных закладок, ошибок и некоторых возможностей компьютерных систем и сетей.

АЛГОРИТМИЧЕСКИЕ КОМПЬЮТЕРНЫЕ УГРОЗЫ

- - добывание фактографической и индексно-ссылочной информации путем поиска, сбора и анализа структурируемой и неструктурируемой информации из общедоступных ресурсов или конфиденциальных источников компьютерных систем и сетей.

СЕМАНТИЧЕСКИЕ КОМПЬЮТЕРНЫЕ УГРОЗЫ

- - добывание данных путем внедрения и применения вредоносных программ в уже эксплуатируемые программные комплексы и системы для перехвата управления компьютерными системами.

ВИРУСНЫЕ КОМПЬЮТЕРНЫЕ УГРОЗЫ

- добывание информации из отдельных (локальных) компьютерных систем, возможно и не входящих в состав сети, на основе преодоления средств разграничения доступа, а также реализация несанкционированного доступа при физическом доступе к компьютеру или компьютерным носителям информации.

РАЗГРАНИЧИТЕЛЬНЫЕ КОМПЬЮТЕРНЫЕ УГРОЗЫ

СЕТЕВЫЕ КОМПЬЮТЕРНЫЕ УГРОЗЫ

- - добывание данных из компьютерных сетей, путем анализа уязвимостей сетевых ресурсов (и объектов пользователей) и последующего удаленного доступа к информации, а также блокирование доступа к ним, модификация, перехват управления либо маскирование своих действий.

- - добывание информации и данных путем перехвата, обработки и анализа сетевого трафика (систем связи) и выявления структур компьютерных сетей и их технических параметров.

ПОТОКОВЫЕ КОМПЬЮТЕРНЫЕ УГРОЗЫ

АППАРАТНЫЕ КОМПЬЮТЕРНЫЕ УГРОЗЫ

- - добывание информации и данных путем обработки сведений, получения аппаратуры, оборудования, модулей и их анализа, испытания для выявления их технических характеристик и возможностей, полученных другими типами ТКУ.

- добывание информации и сведений путем "вертикальной" обработки, фильтрации, декодирования и других преобразований форматов (представления, передачи и хранения) добытых данных в сведения, а затем в информацию для последующего ее представления пользователям.

ФОРМАТНЫЕ КОМПЬЮТЕРНЫЕ УГРОЗЫ

МЕТОДЫ РЕАЛИЗАЦИИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПО УРОВНЯМ

ТИТУЛЬНЫЙ

Уровни доступа к информации	**Основные методы реализации угроз информационной безопасности**			
	Угроза раскрытия параметров системы	Угроза нарушения конфиденциальности	Угроза нарушения целостности	Угроза нарушения доступности
Носителей информации	Определение типа и параметров носителя информации	Хищение (копирование) носителей информации, перехват ПЭМИН	Уничтожение машинных носителей информации	Выведение из строя машинных носителей информации
Средств заимствования с носителем	Получение информации о программно-аппаратной среде, получение детальной информации о функциях, выполняемых системой	Несанкционированный доступ к ресурсам системы, совершение пользователем несанкционированных действий.	Внесение пользователем несанкционированных изменений в программы и данные, установка и использование нештатного программного обеспечения	Проявление ошибок проектирования и разработки программно-аппаратных компонентов системы.
Представления информации	Определение способа представления информации	Раскрытие представленной информации (дешифрование)	Внесение искажения в представлении данных	Искажение соответствия синтаксических и семантических конструкция языка
Содержания информации	Определение содержания данных на качественном уровне	Раскрытие содержания информации	Введение дезинформации	Запрет на использование информации.

ПОЛЬЗОВАТЕЛЬСКИЕ КОМПЬЮТЕРНЫЕ УГРОЗЫ

- - добывание информации о пользователях, их деятельности и интересах на основе определения их сетевых адресов, местоположения, организационной принадлежности, анализа их сообщений и информационных ресурсов.

ЗАКЛЮЧЕНИЕ

- Объектами защиты от технических компьютерных угроз являются: компьютерные системы (сети) и характеристики их пользователей и программно-аппаратных средств. Выделено 9 типов угроз: семантических, алгоритмических, вирусных, разграничительных, сетевых, потоковых, аппаратных, форматных и пользовательских. Необходимо особо отметить, что все эти 9 типов компьютерных угроз просто необходимо учитывать при обеспечении безопасности информации в системах информационных инфраструктур.

ИСПОЛЬЗУЕМАЯ ЛИТЕРАТУРА

https://pirit.biz/reshenija/informacionnaja-bezopasnost

https://habr.com/ru/company/vps_house/blog/343110/

https://searchinform.ru/informatsionnaya-bezopasnost/

https://www.sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema1