ВВЕДЕНИЕ

Актуальность исследования.

Актуальность обеспечения информационной безопасности телекоммуникационных систем возрастает в связи с рядом объективных причин. Одна из них это высокий уровень популярности ИТКС, которым доверяют самую ответственную работу, от качества которой зависит жизнь и благосостояние многих людей. При этом ИТКС, открывая новые возможности в организации человеческой деятельности, повышения ее качества и эффективности, в то же время становятся одной из наиболее уязвимых компонент, притягивая к себе злоумышленников, как изнутри, так и из вне [3].

Сегодня с помощью ИТКС в электронном режиме может производиться учет, открывать кредиты, переводиться значительные суммы, поэтому незаконное манипулирование информацией подобного характера может привести к серьезным ущербам. Кроме того, данные циркулирующие в ИТКС, затрагивают интересы большого количества юридических и физических лиц. Как правило, информация конфиденциальна. В то же время она должна быть доступна и актуальна, что обуславливает существенную ответственность ИТКС за обеспечение вышеуказанных качеств информации [48, 25].

Всплеск многообразия используемых системно-технических платформ и номенклатуры сетевых сервисов приводит к расширению списка уязвимостей ИТКС и повышает требования к средствам их защиты. Установка в ИТКС стандартных средств защиты таких, как межсетевые экраны, виртуальные частные сети, средства защиты от несанкционированного доступа и пр. является необходимым, но уже не достаточным условием построения надежной и эффективной безопасности [25, 28].

Отсюда вытекает необходимость снижения уровня риска ИТКС от реализации внутренних и внешних угроз и, в конечном счете, минимизации ущерба от деструктивных деяний. В такой ситуации базовой процедурой является риск-анализ, который позволит всесторонне исследовать атакуемые

ИТКС организации, оценить текущий уровень состояния ИБ, выявить уязвимые места в системе защиты, создать модели возможных угроз ИТКС, проверить правильность подбора и настройки средств защиты при реализации атак [48].

В результате риск-анализа ИТКС выявляются уязвимые технологические потоки как электронной, так и бумажной информации, топологии сети, незащищенные или неправильные сетевые соединения, производится анализ настроек межсетевых экранов и других средств защиты. Целью проведения такого анализа является разработка ряда методик, моделей и организационных документов, которые в дальнейшем могут явиться основой для построения защищенной ИТКС.

В этой связи чрезвычайно актуальной является задача нахождения универсальных методик и алгоритмов управления информационными рисками, базирующихся на анализе возможного ущерба ИТКС от ожидаемых атак [3].

Сетевые атаки на ИТКС, вредоносными программами –ее тевые черви" становятся панацеей нынешнего времени.

Любая ИТКС может выступать в качестве объекта информационной атаки, которая может быть определена как совокупность действий злоумышленника, направленная на нарушение одного из трѐх свойств информации - конфиденциальности, целостности или доступности. Рассмотрим эти свойства более подробно. Свойство конфиденциальности позволяет не давать права на доступ к информации или не раскрывать ее неполномочным лицам, логическим объектам или процессам [38].Характерным примером нарушения конфиденциальности информации является кража из системы секретной информации с целью еѐ дальнейшей перепродажи. Целостность информации подразумевает еѐ способность не подвергаться изменению или уничтожению в результате несанкционированного доступа. В качестве примера нарушения этого свойства можно привести ситуацию, при которой злоумышленник

преднамеренно искажает содержимое одного из электронных документов, хранящихся в системе [5]. И, наконец, доступность информации определяется как еѐ свойство быть доступной и используемой по запросу со стороны любого уполномоченного пользователя. Таким образом, в результате нарушения конфиденциальности, целостности или доступности информации злоумышленник тем самым может нарушить бизнес-процессы компании[1,4].

Основной ущерб в ИТКС от атак вредоносных программ «сетевые черви» является потеря информации, документов, баз данных, программного обеспечения, видео-аудио и тд., то есть риском является полное или частичное уничтожение данных.

Одни из первых экспериментов по использованию компьютерных червей в распределѐнных вычислениях были проведены в исследовательском центре Xerox Альто Джоном Шочем (John Shoch) и Йоном Хуппом (Jon Hupp) в 1978 году. Термин возник под влиянием научно-фантастических романов Дэвида Герролда «Когда ХАРЛИ исполнился год» и Джона Браннера «На ударной волне» [5].

Зачастую «сетевые черви» даже безо всякой полезной нагрузки перегружают и временно выводят из строя сети только за счѐт интенсивного распространения. Типичная осмысленная полезная нагрузка может заключаться в порче файлов на компьютере-жертве, также из зараженных ИТКС возможна организация ботнета для проведения сетевых атак[5,13].

Одним из наиболее известных компьютерных червей является «Червь Морриса», написанный Робертом Моррисом-младшим, который был в то время студентом Корнельского Университета. Распространение червя началось 2 ноября 1988, после чего червь быстро заразил около 10 % всех компьютеров, подключѐнных в то время к Интернету [38].

Актуальность данной работы заключается в разработке методики оценки рисков при воздействие на ИТКС атак вредоносными программами

«сетевой червь», а также выработка предложений об увеличении эффективности существующих механизмов противодействия данным атакам.

Степень научной разработанности.

В настоящее время активно ведутся исследования возможности применения, для обеспечения информационной безопасности различных автоматизированных систем, риск-моделей различных атак на компоненты распределенных систем и возникающих от их реализации ущербов[3]. Многовариантность и непредсказуемость таких атак не позволяют создать детерминированное описание описания этих процессов и возникающих от их реализации ущербов. Поэтому, при создании защищенных автоматизированных систем, вполне обоснованно рассмотрение ущерба как случайной величины. В этом случае описание принято осуществлять с использованием различных законов распределения, среди которых наибольшей популярностью пользуются регулярные законы [93].

Таким образом, исходя из актуальности и степени научной разработанности данной проблемы, можно сделать вывод о целесообразности проведения комплексных исследований в данном направлении.

Объект исследования. Объектом исследований является распределенная локальная вычислительная сеть, как цель программно-математического воздействия типа «сетевые черви».

Предмет исследования.Методы оценки и регулирования рисков в распределенной локальной вычислительной сети, являющихся целью атак, направленных на реализацию программно-математического воздействия типа «сетевые черви».

Цель и задачи исследования.

Целью настоящей работы является исследование и разработка подходов для оценки и регулирования рисковвраспределенной локальной вычислительной сети, подвергающихся угрозам программно-математического воздействия типа «сетевые черви».