ВВЕДЕНИЕ

Актуальность исследования

Информационная безопасность предприятия – это защищенность информации, которой располагает предприятие (производит, передает или получает) от несанкционированного доступа, разрушения, модификации, раскрытия и задержек при поступлении. Информационная безопасность включает в себя меры по защите процессов создания данных, их ввода, обработки, и вывода.[2,3]

Целью комплексной информационной безопасности является сохранение информационной системы предприятия в целости и сохранности, защита и гарантирование полноты и точности выдаваемой ею информации, минимизация разрушений и модификация информации, если таковые случаются.[2,4,6]

Одной из важнейших проблем национальной безопасности страны является обеспечение информационной безопасности и защиты информации в специализированных организациях военно-стратегического назначения.[44] К специализированным организациям военно-стратегического назначения Министерства обороны относятся работающие на оборонный заказ предприятия военно-научного сопровождения разработки государственных программ обороноспособности страны, систем вооружения, стратегических ударных средств, космических комплексов и средств ракетно-космической обороны, систем боевого управления стратегическими ядерными силами и другие специализированные научные организации, имеющие особый режим безопасного функционирования и охраны государственной тайны. [4,6,71]

Оборонное предприятие создает сложную продукцию и образцы вооружения. Из-за этого в кооперации по производству входят до 1,5-2 тысячи предприятий. Образец создается на одном «головном» предприятии, поэтому это предприятие вынуждено использовать открытые телекоммуникационные сети, для оформления соответствующих договорных отношений, необходимых для реализации производственного изделия.[61,78]

Следует отметить, что в условиях рыночной экономики деятельность этих ранее

полностью засекреченных и зачастую градообразующих организаций несколько изменилась. В настоящее время предприятия и организации, на которые законодательством РФ возложены функции оперативно-стратегического и военно-экономического обоснования разработки и сопровождения научно-технической продукции оборонного назначения, являются юридическими лицами в форме государственных унитарных (федеральных казенных) предприятий (ГУП) на праве хозяйственного ведения либо оперативного управления. [2,6,90] Эти предприятия созданы на базе ликвидированных федеральных государственных предприятий Министерства обороны и являются их правопреемниками. (Это касается ранее выделенных федеральных средств, отношений землепользования, природопользования, использования недр, предоставления квот и лицензий и др.).[4,71]

Правовой основой реорганизации особо защищаемых объектов национальной безопасности страны послужило следующее. Конституцией Российской Федерации 1993 года управление федеральной собственностью отнесено к компетенции Правительства РФ. В соответствии с этим Правительство Российской Федерации приняло Постановление от 10 февраля 1994 г. N 96 «О делегировании полномочий Правительства Российской Федерации по управлению и распоряжению объектами федеральной собственности». [37] Согласно этому постановлению решение о создании или ликвидации государственных федеральных предприятий принимается Правительством Российской Федерации на основании совместного представления федеральных органов исполнительной власти — Министерства имущественных отношений Российской Федерации, Министерства экономического развития и торговли и отраслевого федерального органа исполнительной власти.[74,78]

Правовое положение унитарного предприятия, основанного на праве оперативного управления (федерального казенного предприятия) весьма специфично и несколько «уже» права хозяйственного ведения. Федеральное казенное предприятие создается на базе федерального имущества по особому решению Правительства Российской Федерации.[37,94] При этом федеральные

экономики, не имеющих непосредственного отношения к деятельности специализированных структур. [2,45]

Компьютеризация, развитие телекоммуникаций предоставляют сегодня широкие возможности для автоматизированного доступа к различным конфиденциальным , персональным и другим важным, критическим данным в обществе (его граждан, организаций и т.д.). [83]

Все это в совокупности формирует такой фон политического и социально-экономического положения организаций военно-стратегического назначения, на котором вполне естественными кажутся противоречия между обеспечением выполнения функций, ради которых были образованы специализированные объекты, необходимостью защиты государственных секретов в этих особо важных для государства организациях и расширением свободного обмена информацией, а так же крайне широкие возможности для конкурентов и злоумышленников.[78,63,2] Из этого очевидно, насколько актуален в наши дни вопрос с защитой информационных систем на оборонных предприятиях.

Предметом исследования является математическая модель построения опасности, используя теорию случайных импульсных потоков, риск модель в которых формируется на основе совпадения потока штатных переговоров с потоком переговоров злоумышленников.

Объектом исследования являются оборонные предприятия, и их кооперации, распределенные на расстоянии.

Цель и задачи исследования.

Целью работы является разработка математической модели оценивания опасности угроз, действующих на открытые телекоммуникационные сети. В этих сетях появляются новые угрозы, обладающие новизной, таковые, как недобросовестные конкуренты, злоумышленники, способные ввести в заблуждение и произвести фиксацию служебной информации.

В качестве количественной меры оценивания опасности предлагается использовать значения вероятности совпадений попыток реализации указанных

выше угроз в ходе ведения служебных переговоров при реализации и изготовления изделия.

Для достижения такой цели необходимо решить следующие задачи:

1. Разработать описательную модель предприятия на этапе его функционирования при организации кооперации производителей и подготовке производства.
2. Разработать подход для формирования поля угроз для открытых телекоммуникационных сетей в динамике функционирования предприятия.
3. Разработка математической модели оценки безопасности угроз в открытых телекоммуникационных сетях.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в дипломной работе обеспечивается корректным использованием математических методов в приложении обозначенному предмету исследования.

Методы исследования

Для решения поставленных задач необходимо использовать методы системного анализа, теории риска, теории вероятности и математической статистики.

На защиту выносятся следующие основные положения работы:

1. Математические модели форматов поступающих данных, исходящих данных на этапе подготовки производства.
2. Аналитические модели угроз, воздействующих на открытые телекоммуникационные сети на оборонном предприятии.
3. Математическая модель оценки безопасности угроз в открытых телекоммуникационных сетях.

Научная новизна исследования.

Научная новизна исследования заключается в разработке более подробного представления угроз недобросовестной конкуренции и введение в заблуждения, а так же построение математической риск/шанс модели, основанной полностью на случайных импульсных потоках.