ВВЕДЕНИЕ

Актуальность

Проблема информационной безопасности постоянно усугубляется процессами проникновения практически во все сферы деятельности общества технических средств обработки и передачи данных.На любом, даже самом маленьком предприятии, присутствуют средства вычислительной техники, используемые для обработки информации. Нарушение целостности, уничтожение или хищение данных, приводит к причинению ущерба различной степени для организации, что приводит к экономическим убыткам. А если учесть тот факт, что вредоносные программы развиваются параллельно с всеобщей информатизацией, защита автоматизированных систем должна рассматриваться как необходимая мера безопасности.

Информационная безопасность достигается путем реализации соответствующего комплекса мероприятий по управлению информационными рисками [39]. Посредством оценки рисков происходит выявление угроз активам организации, оценка уязвимости соответствующих активов и вероятности возникновения угроз, а также оценка возможных последствий.При неправильном расчете рисков организации есть вероятность понести огромный ущерб, как количественный (потеря прибыли), так и качественный (потеря доверия к организации)[15, 28].

Среди всего многообразия вредоносных программ, выделяется большой класс троянских вирусов. Среди них есть подклассTrojan-Ransom, которому до сих пор уделяется мало внимания, но который способен заблокировать работу операционной системы, несмотря на установленные на ней антивирусные программы.

Троянскими программами (троянскими конями) обычно называют программы, содержащие скрытый модуль, осуществляющий несанкционированные действия.

Эти действия не обязательно могут быть разрушительными, однако практически всегда направлены во вред пользователю[14, 23].

В настоящее время были изучены: вопросы воздействия троянов на АС (дипломные работы Рудакова Е.В и Тонких Н К); вопросы применимости степенного закона распределения для оценки рисков АС; вопросы противодействия вирусным атакам; вопросы проникновения Trojan-Ransomв АС.

В изученных источниках литературы по проблематике не исследованы: вопросы оценки ущербов программ Trojan-Ransom; вопросы построения адекватной математической модели риск-анализа АС при воздействии этого вируса; вопросы минимизации ущерба от воздействия Trojan-Ransom; вопросы оценки экономической эффективности мер информационной защиты от программ Trojan-Ransom.

В дипломной работе проведен риск-анализ автоматизированной системы при воздействии на нее Trojan-Ransom.

Одна из разновидностей троянских программ – троянцы-вымогатели (Trojan-Ransom [23]) – вредоносное ПО, нарушающее работоспособность компьютера посредством полной или частичной блокировки операционной системы или шифрования файлов и вымогающее деньги у пользователей за их восстановление.

После заражения компьютера вредоносные программы Trojan-Ransom, в зависимости от функционала, блокируют доступ к веб-сайтам, шифруют на зараженном компьютере файлы определенных форматов или полностью блокируют доступ к системе.

В связи с этим анализ программ Trojan-Ransom является в настоящее время актуальным. В дипломном проекте рассматриваются вопросы, связанные с

особенностями функционирования и реализации деструктивных функций программ Trojan-Ransom.

Цель работы построение вероятностной модели воздействия троянских атак Trojan-Ransomна автоматизированные системы, а также разработка алгоритма оценки и управления возникающими в данном случае информационными рисками автоматизированной системы.

Для достижения поставленной цели в дипломной работе необходимо решить следующие задачи:

1. Рассмотреть различные модификации исследуемой «Троянской программыTrojan-Ransom» и способы их проникновения в автоматизированную систему.
2. Разработать вероятностные модели ущербов от воздействия троянской программы на автоматизированную систему.
3. Разработать алгоритм минимизации рисков при воздействии программ Trojan-Ransom
4. Произвести оценку экономической эффективности, а также расчет сметной стоимости и договорной цены проведенного исследования;

Объектом исследования являетсяавтоматизированная система, подвергающаяся троянским атакам.

Предметом исследования является статистический риск-анализ деструктивных воздействий троянских атак Trojan-Ransom, а так же организационные меры противодействия им.

Методы исследования

Для решения поставленных задач исследования в ходе выполнения работы применялись методы теории вероятностей, математической статистики, теории математического моделирования, теории рисков, теории чувствительности рисков, теории оптимального управления и теории нелинейного программирования.

ЗАКЛЮЧЕНИЕ

1. На основе проведенных в дипломной работе исследований разработана вероятностная модель ущербов при воздействии программы Trojan.Ransom, позволяющая представить закономерности функционирования «трояна», и алгоритм минимизации рисков, позволяющий количественно оценить ущерб от деструктивного воздействия на автоматизированную систему.

2. В ходе работы выдвинута оригинальная научная гипотеза интегральной оценки ущерба на основе рассмотрения двух вариантов атак: синхронного и асинхронного.

3. В дипломной работе доказана перспективность предлагаемых идей для практического применения. Как показано в ходе исследования, применения изложенного алгоритма минимизации позволит повысить экономическую эффективность.

4. В ходе исследования было уточнено понятие интегральной оценки риска.

5. При проведении исследовании было доказано положениео применимости степенного распределения для моделирования воздействия троянской программы и расширены границы применимости вероятностной модели, основанной на степенном распределении, на область исследований программ Trojan.Ransom.

6. Эффективно использован метод теории вероятности, математической статистики, управления рисками: получена вероятностная модель ущербов и алгоритм минимизации рисков при воздействии программ Trojan.Ransom.

7. В дипломной работе изложены положения теории математической статистики о получении статистических характеристики случайных величин, теория вероятности, теория оценки рисков и экономическая теория.

8. В ходе исследований выявлено противоречие между интенсивным ростом количества модификаций программы Trojan.Ransom и отсутствием информированности персонала, обслуживающего автоматизированную систему, об угрозе, представляемой вирусом Trojan.Ransom, и необходимых мерах защиты от атак программ этого класса.