Содержание

Введение

Для современного этапа развития общества характерен непрерывный процесс информатизации и совершенствования информационных технологий. С внедрением информационных технологий во все сферы жизнедеятельности человека проблемы информационной безопасности (ИБ) с каждым годом становятся всѐ более сложными и многогранными. Область применения автоматизированных информационных систем (АИС) также не является исключением и постоянно расширяется, затрагивая организацию деятельности в различных сферах жизни общества [4, 5].

Открывая новые возможности перед человеком в модернизации различных технологических и управленческих процессов, повышении качества и эффективности работы, на АИС возлагается существенная ответственность за сохранность и безопасность информации. Для правильной работы АИС осуществляется телекоммуникационное и информационное взаимодействие подсистем различного назначения (общего пользования, частных, производственных, ведомственных). Поддержание взаимодействия отдельных территориально-распределенных подсистем внутри каждой из систем, а также между отдельными системами АИС происходит посредством постоянного предоставления услуг информационного и аналитического характера, обеспечения информационной безопасности, администрирования единого информационного пространства и средств безопасности. Временная недоступность критически важного узла АИС или его несанкционированное использование может не только нанести владельцу системы значительный материальный ущерб, но и привести к экологической или техногенной катастрофе. Таким образом, необходима реализация эффективной политики безопасности, согласующей средства защиты всех узлов и подсистем АИС, а информация, циркулирующая в системе, должна быть не только актуальна и доступна, но и защищена от воздействия злоумышленников как изнутри, так и из вне[6, 8, 15].

Уязвимость АИС существенно превышает уязвимость отдельно взятых узлов.

Это связано, прежде всего с масштабностью и неоднородностью самих автоматизированных информационных систем. При этом число угроз информационной безопасности и способов их реализации постоянно растет. Основными причинами являются здесь рост сложности программно- аппаратных средств и недостатки современных информационных технологий. С учетом того, что любая АИС в той или иной части имеет доступ к сети Интернет, наиболее актуальными угрозами безопасности на сегодняшний день являются угрозы распространения вредоносной информации через сеть. Интернет является идеальной средой для распространения вредоносного программного обеспечения, т.к. он обеспечивает огромное число подключенных рабочих станций иширокий канал распространения вредоносного программного обеспечения[6, 18].

Одним из популярных и действенных способов реализации распространения вредоносной информации является использование почтового вируса-червя, который обладает способностью к несанкционированному саморазмножению по каналам электронной почты. В связи с тем, что электронная почта является одной из наиболее популярных и востребованных во всем мире информационных услуг, которая позволяет осуществлять пересылку, обработку информации, поддерживать оперативную связь между пользователями, атаки с использованием почтового червя наносят огромный ущерб различным АИС.В процессе размножения червь отсылает либо свою копию в виде вложения в электронное письмо, либо ссылку на свой файл, расположенный на каком-либо сетевом ресурсе, что активизирует код червя. Злоумышленник получает возможность распространения вредоносной информации в АИС, что ведет к нарушениям и сбоям в работе АИС. В связи с этим важнейшей задачей является обеспечение достаточной степени защищенности подсистем АИС для их эффективного функционирования в условиях проявления внутренних и внешних информационных угроз и, в конечном счете, минимизации ущерба от деструктивных деяний. Изучение угроз информационных воздействий вируса-червя почтовых червей в АИС и методов противодействия им – крайне актуальная задача. Для решения такой задачи требуется исследованиямножества факторов, влияющих наживучесть АИС. Одним из таких факторов является полнота и точность

разработанноймодели ущерба от реализации атак с использованием почтовых червей [4, 5, 8, 9].

Модель — это материальный или мысленно представляемый объект, который в процессе изучения замещает объект, сохраняя его важные для данного исследователя типичные черты. При помощи построенной модели выявляются наиболее существенные факторы, формирующие те или иные свойства объекта. Существуют различные методы моделирования, имеющие свои достоинства и недостатки. Наиболее востребованными являются методы детерминированного, стохастического, статического, дискретного моделирования. Однако каждый из методов моделирования имеет не только свои уникальные достоинства, но и недостатки. Для того, чтобы повысить точность результатов моделирования и описать моделируемый процесс с большей адекватностью, необходимо синтезировать несколько методов моделирования и получить новую, уникальную модель ущерба от атак с использованием почтовых червей [27, 32].

Таким образом, построение актуальной и всесторонней синтезированной модели позволит не только уменьшить возможный ущерб от успешной атаки с использованием почтового червя и увеличить эффективность используемых средств защиты, но и позволит повысить живучесть АИС в целом и в отдельных узлах [4, 29, 30].

Степень проработанности темы

В настоящее время активно ведется изучение атак, основанных на использовании почтовых червей и исследование по разработке моделейущерба от их реализации с целью обеспечения информационной безопасности АИС. Непредсказуемость таких атак не позволяет создать детерминированное описание этих процессов и возникающих от их реализации ущербов. Поэтому, при создании защищенных АИС, вполне обоснованно моделирование ущерба от реализации атак, основанных на использовании почтовых червей как случайной величины.

Таким образом, исходя из актуальности и степени научной разработанности проблемы нарастания ущерба реализации атак, основанных на использовании почтовых червей, можно сделать вывод о целесообразности проведения

комплексных исследований в направлении построения синтезированной аналитической модели ущерба и изучения живучести системы.

Объектом исследования являются рабочие станции автоматизированной информационной системы, в отношении которых реализуется атака с использованием почтовых червей.

Предметом исследования является синтезированная аналитическая модель ущерба автоматизированной информационной системы, в отношении которой реализуются атаки с использованием почтовых червей.

Цели и задачи исследования.

Цель настоящей работы заключается в разработке синтезированной аналитической модели ущерба автоматизированной информационной системы как объекта защиты от деструктивных воздействий атак с использованием почтовых червей. Для достижения указанной цели предполагается решить следующие задачи:

1. Построить аналитическую модель автоматизированной информационной системы как среды реализации атаки с использованием почтового червя;
2. Исследовать поэтапный процесс реализации атаки с использованием почтовых червей;
3. Разработать функции ущерба реализации атаки с использованием наиболее актуальных почтовых червей;
4. Исследовать стратегии распространения почтовых червей в автоматизированной информационной системе;
5. Разработать стратегии иммунизации для различных моделей инфицирования почтовыми червями автоматизированной информационной системы;
6. Осуществить имитационное моделирование функции ущерба с выработкой практических рекомендации по снижению информационных рисков;
7. Провести оценку динамикиразличных стратегий иммунизации для различных стратегий инфицирования в автоматизированной информационной системе.

8. Провести оценку экономической эффективности проведенного исследования;

9. Проанализировать возможные проблемы с учетом обеспечения безопасности жизнедеятельности.

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

В исследовании предполагается использовать методы теории вероятности, методы математической статистики и статистического анализа, методы теории графов, методы теории Петри – Маркова, методы аналитического моделирования, методы теории рисков [12, 13, 26, 32].

Научная новизна исследования.

В настоящей работе получены следующие основные результаты, характеризующиеся научной новизной:

1. В исследовании основных угроз, связанных с работой автоматизированных информационных систем, были учтены результаты их количественного и качественного развития, а также особенности реализации атак с использованием наиболее актуальных почтовых червей.

2. В отличие от аналогичных работ, полученная модель ущерба реализации атаки с использованием почтового червя включает учет различных стратегий инфицирования.

3. Отличительной особенностью подхода к изучению безопасности автоматизированных информационных систем, в отношении которых реализуются атаки с использованием почтовых червей является изучение динамики стратегий иммунизации для различных стратегий инфицирования.

Практическая ценность работы заключается в том, что:

1. Анализ основных видов угроз, воздействующих на компоненты автоматизированных информационных систем, позволяет выявить наиболее опасные

их виды и дает возможность уделить особое внимание защите от атак с использованием почтовых червей.

2. Построенная синтезированная модель отражает этапы распространения почтового червя с различными стратегиями инфицированияи позволяет всесторонне оценивать процесс развития атаки.

3. Полученные выражения для оценки стратегий иммунизации автоматизированных информационных системпозволяют оценить эффективность обеспечения защиты от реализации атак с использованием почтовых червей.