УДК 004.7

К.Ю. Заруба
Донецкий национальный технический университет, г. Донецк
кафедра систем искусственного интеллекта

АНАЛИЗ МЕТОДОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация

Заруба К.Ю. Анализ методов обеспечения информационной безопасности. *Проведён анализ информационных процессов, протекающих в компьютерных средах. Систематизированы современные информационные угрозы применительно к интеллектуальным системам, их информационной инфраструктуре и компьютерной среде, в которой они находятся, и определены основные тенденции развития угроз. Разработан ряд организационных и технических мероприятий по защите информационных систем.*

Ключевые слова: *информационная безопасность, информационная система, инфраструктура информационной системы, компьютерные угрозы, модель защиты.*

Постановка проблемы. Защита информационных систем направлена на обеспечение сохранности рабочих данных, бесперебойного функционирования компьютеров, программного обеспечения и операционной системы. Возрастающая роль информационной безопасности в сфере информационных систем обуславливает необходимость расширения научных исследований не только в рамках информационной безопасности ИС, но в области ее инфраструктуры. Проблема заключается в построении алгоритмов позволяющих повысить защищенность информационной структуры.

Цель статьи – исследование организационно-технологических особенностей обеспечения информационной безопасности ИС и ее информационной инфраструктуры, позволяющих повысить защищенность информационной инфраструктуры ИС от внешних и внутренних угроз.

Решение проблемы и результаты исследований. Информационная среда и информационные ресурсы являются важным фактором жизнедеятельности современного общества. Эта совокупность включает коллекции информации, информационные потоки, информационные объекты, информационные инфраструктуры, а также системы регулирования возникающих при этом общественных отношений. Все более повышается роль субъектов, осуществляющих сбор, формирование, распространение и использование информации. Информационные угрозы для информационных

систем (ИС) имеют устойчивую тенденцию к росту и модифицируемости. К настоящему времени в области обнаружения вторжений в информационные системы преобладает подход обнаружения злоупотреблений, который основан на построении модели атаки непосредственно на систему ИС. Однако, данный подход имеет очевидный недостаток, связанный, прежде всего, с недостаточным учетом влияния инфраструктуры и компьютерной среды [1].

В настоящее время большой интерес представляет динамика уязвимостей по типам воздействия. На рисунке 1 приведены уязвимости по типам воздействия на систему.

Для анализа использованы статистические данные, публикуемые в печати и Интернет, например, фирмой Semantek [2]. Как следует из рис.1 одной из основных угроз является получение доступа к системе. Эта угроза чаще реализуется эвристическими методами двухходовыми или многоходовыми атаками.

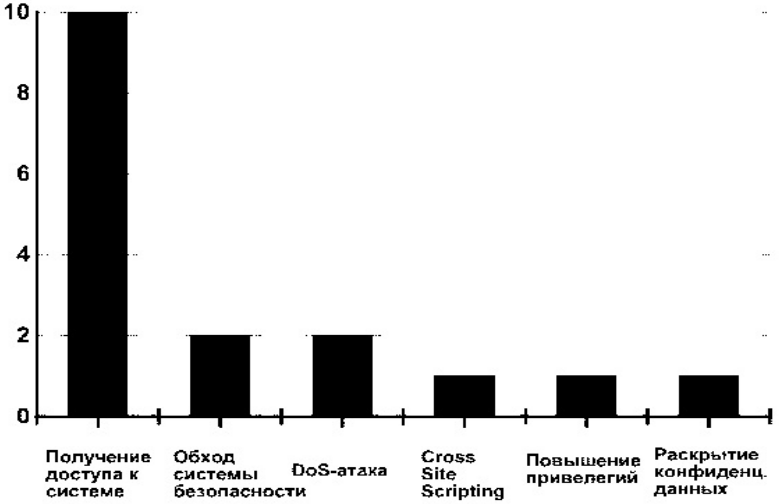

Рисунок 1 – Статистика уязвимостей по типу воздействия на систему

Существуют информационные отношения между информационной системой, ее инфраструктурой и компьютерной средой, в которой они находятся. Наличие информационных отношений предопределяет взаимную связь и необходимость учета этих отношений при организации информационной безопасности.

Инфраструктура информационной системы (Information Infrastructure Systems – IIS) включает совокупность интерфейсов, систем обмена, информационных центров, систем связи и обеспечивает доступ потребителей к информационным ресурсам ИС.

На основе функционального подхода можно построить модель компьютерной среды и информационной инфраструктуры ИС, которая представлена на рис.2. Компьютерная среда является основой функционирования ИС. Большинство информационных взаимодействий осуществляется через инфраструктуру ИС.

Рисунок 2 – Компьютерная информационная среда и инфраструктура информационной системы

Наибольшие уязвимости ИС и компьютерной среды связаны с информационными сетевыми взаимодействиями и с работой пользователя [3].

В таблице 1 показаны основные угрозы, характерные для информационной системы и ее инфраструктуры. Единица означает наличие угрозы, ноль - отсутствие угрозы.

Таблица 1 – Основные угрозы для ИС и ее информационной инфраструктуры

	Вид угрозы	Объект воздействия	
		ИС	ИИИС
1.	Неумышленные ошибочные действия собственных сотрудников	1	1
2.	Сбои оборудования	1	1
3.	Попытки внешнего несанкционированного доступа	0	1
4.	Умышленные ошибочные действия собственных сотрудников	1	1
5.	Атаки через сеть	0	1
6.	Ошибочные исходные данные	1	0
7.	Сбои программного обеспечения	1	1
8.	Нарушение согласования ИС с внешней системой	0	1
9.	Нарушение изменения режима секретности или доступа	0	1

Из таблицы следует, что ИС практически принимает все внешние угрозы на себя. Отсюда еще раз вытекает важность организации информационной безопасности ИС, как первоочередной задачи информационной безопасности ИС.

Существуют четыре основные модели информационной безопасности: Биба, Гогена-Мезингера, Кларка-Вильсона и Сазерлендская модели. Общий недостаток всех рассмотренных моделей – апостериорный подход. Они защищают информационные системы после их создания. Для устранения этого недостатка при построении модели защиты необходимо учитывать предположение о том, что понятие информационной безопасности IIS шире, чем понятие безопасности ИС. Это приводит к необходимости включения в параметры защиты IIS дополнительных параметров и показателей, отражающих защищенность компьютерной среды. К таковым относятся не только защищенность, но и качество проектирования, среды, надежность функционирования и другие факторы. Проектная модель защиты представлена на рис.3.

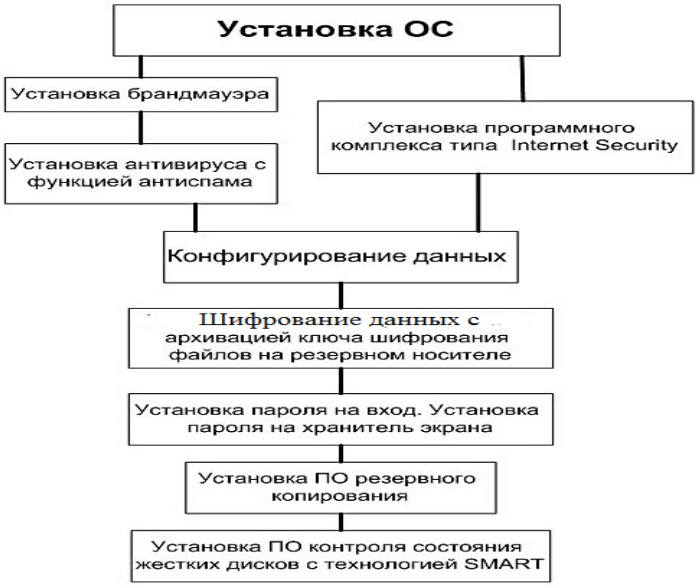

Рисунок 3 – Проектная модель защиты

Выводы. Проведён анализ информационных процессов, протекающих в компьютерных средах. Данные исследования показали, что многие практикуемые методы защиты информации не учитывают особенности инфраструктуры информационных систем, не рассматривают ее как объект первоочередной защиты, не предлагают комплексных решений по организации защиты в системе ИС+инфраструктура. Поэтому существует необходимость в создании алгоритмов и рекомендаций, повышающих информационную безопасность ИС и работу с ИС, таких как борьба со спамом и компьютерными шпионами.

Список литературы

1. Галатенко В.А. Основы информационной безопасности. – Учебное пособие. – Интернет-университет информационных технологий, 2006 – 208с.
2. Официальный сайт Symantec. Отчет об угрозах безопасности в Интернете [Електронный ресурс]. – Режим доступа: http://www.symantec.com/ru/ru/threatreport
3. Методы и средства анализа рисков и управление ими в ИС [Електронный ресурс]. – Режим доступа: http://www.bytemag.ru/articles