УДК 004.056.53

А.О. Шемяков

Причины повышения уязвимости и снижения стойкости функций безопасности автоматизированных систем вуза

На основе комплексного подхода рассматриваются основные причины повышения уязвимости и снижения стойкости функций безопасности автоматизированных систем высшего учебного заведения. Приводится анализ последствий автоматизации процессов обеспечения безопасности и связанных с ней изменений системы «система защиты – объект защиты».

Ключевые слова: автоматизированная система, защита информации, объект защиты, информационная безопасность.

Следствием применения автоматизированных систем (АС) является взаимная интеграция объекта информатизации и системы защиты. Лежащие в основе этой интеграции современные информационные технологии с каждым годом все больше стирают грани различия между первым и вторым. Это обстоятельство выдвигает новые требования к процессам проектирования и разработки систем управления, в том числе и высших учебных заведений. Суть этих требований состоит в необходимости дополнительного учета топологии и свойств объекта защиты. Существующие естественные тенденции к усложнению объектов защиты требуют соответственно создания более сложных АС.

Анализ ретроспективы развития технологий использования АС и перспектив их дальнейшего совершенствования позволяет выявить устойчивую тенденцию интегрирования компьютерных средств и средств связи в рамках нового класса сложных АС – информационно-телекоммуникационных. Это обстоятельство определило вхождение в оборот таких новых понятий, как *информатизация* [6], *изделия информационных технологий*, *объект информатизации* [1], *инфотелекоммуникационная инфраструктура* и многих других. Вместе с тем результатом автоматизации является не только «технический симбиоз» слабо формализуемых систем «объект защиты – система защиты», но и целый ряд связанных с ними новых проблем – проблем информационной безопасности. Большинство из них возникли после осуществления процесса автоматизации и являются его непосредственным следствием [2].

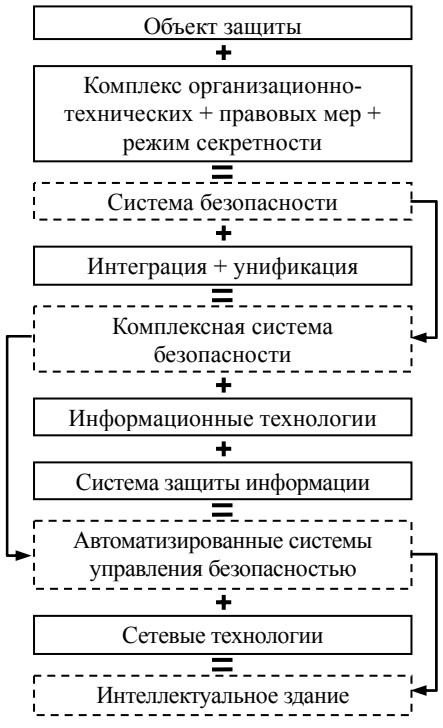

Рис. 1. Обобщенная схема «эволюции» технологий защиты

На рис. 1 показана обобщенная схема совместной эволюции объекта и системы защиты, движущей силой которой является мировой научно-технический прогресс вообще и прогресс современных информационных технологий в частности.

Контрастирующая простота абстрактной схемы «технического симбиоза» системы и объекта защиты 60–70-х годов определяется тем обстоятельством, что на начальном этапе система социальных, экономических, технологических и иных причинно-следственных взаимосвязей в этой сфере деятельности складывалась постепенно. Число такого рода взаимосвязей было невелико и с точки зрения возможности учета их в исследованиях имело незначительный прирост во времени.

Это давало возможность, опираясь на накопленный опыт, легко искать исторические прецеденты, медленно «эволюционно» совершенствовать объект исследований. Актуальность внутренних угроз была незначительной. В настоящее же время многократно возросло число внутренних взаимосвязей. Возникла необходимость учета большого числа причинно-следственных взаимосвязей внешних факторов.

Значительно повысилась разнородность природы и механизмов структурных составляющих системы и объекта защиты. Произошло усиление их интравертности, приведшее к тому, что развитие их подсистем в большей мере стало осуществляться по своим внутренним закономерностям [2].

Возросло число угроз, явившихся следствием автоматизации и включения систем и объектов защиты в пространство современных информационных технологий. Стала актуальной модель внутреннего нарушителя, являющегося продуктом той же самой научно-технической и культурной парадигмы, что и разработчик средств защиты.

В общем случае последствия «проблемных последствий» автоматизации процессов обеспечения безопасности и связанных с ней изменений системы «система защиты – объект защиты» можно сформулировать в следующем виде.

Во-первых, возрос риск принятия неэффективных решений (вероятность несоответствия реально полученных результатов реализованного решения априорно поставленным целям) по вопросам обеспечения безопасности объектов повышенной потенциальной опасности и критических информационных приложений.

В условиях динамично изменяющегося многообразия внешних и внутренних причинно-следственных взаимосвязей, сопровождающих процессы автоматизации и эволюции рассматриваемого класса систем, не всегда, оказывается, бывает достаточно имеющегося опыта, для того чтобы можно было бы судить, насколько дорого и опасно то или иное принимаемое решение [3].

Во-вторых, возросло число угроз, методы осуществления которых базируются на определенных свойствах АС, обеспечивающих безопасность объекта, которые как бы провоцируют появление средств нападения.

Сегодня нарушитель, получив контроль над объектом повышенной потенциальной опасности с «интеллектуальной» (компьютеризированной) системой управления, может трансформировать его энергетические, материальные и информационные ресурсы в уже им управляемые средства для достижения других, более опасных своих целей.

Это становится возможным за счет возрастающего числа недекларированных возможностей, которыми «автоматически» наделяются системы, включаемые в пространство современных информационных технологий.

Задействование скрытых функциональных ресурсов защищаемых АС, т.е. способностей систем или их подсистем выполнять «по совместительству» новые не предусмотренные функции, является основой для существования целого класса новых типов угроз – угроз потери контроля за системой и (или) ее несанкционированного применения.

В-третьих, на фоне развития высоких технологий информационной и общей безопасности возросли уязвимости систем, обеспечивающих эти виды безопасности и уязвимость самого объекта защиты.

Статистические данные по росту числа атак в информационных системах (рис. 2, 3) [7] отчасти являются тому подтверждением.

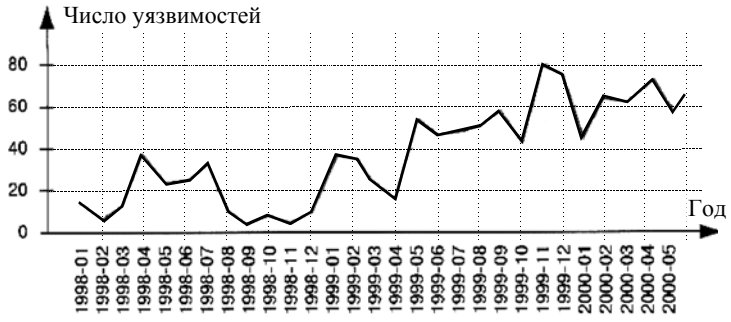

Рис. 2. Современные тенденции изменения числа ежемесячно обнаруживаемых уязвимых мест в программном обеспечении

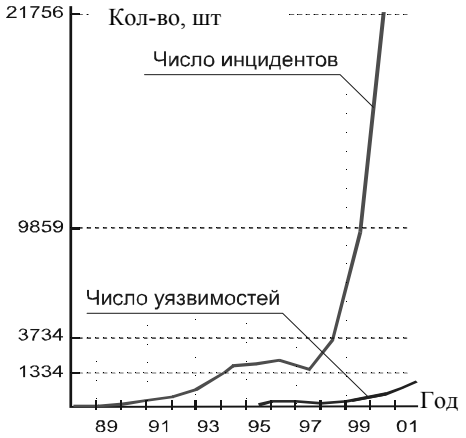

Рис. 3. Статистика роста числа инцидентов и уязвимостей в глобальных сетях передачи данных

Ежегодные отчеты Института компьютерной безопасности – CSI [4:www.gocsi.com] и Координационного центра немедленного реагирования США – CERT [5:www.cert.org] также подтверждают статистку роста числа информационных атак.

Таким образом, автоматизация процесса доступа к информационным ресурсам объекта защиты, в случае нарушения безопасного поведения соответствующей подсистемы защиты, обеспечивает нарушителю возможность воспользоваться этой автоматизацией и «скачать» на магнитный носитель информации в сотни, а то и тысячи раз больше, по сравнению, например, с «традиционными» методами фотокопирования ее с бумажного носителя.

Литература

1. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения [Электронный ресурс]. – Режим доступа: http://vsegost.com/Catalog/86/8680.shtml, свободный (дата обращения: 03.04.2013).

2. Зегжда Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко. – М.: Горячая линия-Телеком, 2000. – 452 с.

3. Лазарев И.А. Информация и безопасность. Композиционная технология информационного моделирования сложных объектов принятия решений. – М.: Московский городской центр научно-технической информации, 1997. – 336 с.

4. Отчет Института компьютерной безопасности – CSI [Электронный ресурс]. – Режим доступа: http://www.gocsi.com, свободный (дата обращения: 02.04.2013).

5. Отчет Координационного центра немедленного реагирования США – CERT [Электронный ресурс]. – Режим доступа: http://www.cert.org, свободный (дата обращения: 03.04.2013).

6. Российская Федерация. Федеральный закон № 24 от 20 февраля 1995 г.: Об информации, информатизации и защите информации. – М., 1995.

7. Сердюк В.А. Криминализация глобальных информационных систем: миф и реальность // Системы безопасности связи и телекоммуникаций. – М.: Гротек, 2000. – № 35. – С. 84–87.

Шемяков Александр Олегович
Ассистент каф. 402 Московского авиационного института
(национального исследовательского университета)
Тел.: 910-423-84-92
Эл. почта: a.shemyakov@gmail.com

Shemyakov A.O.

The reasons of increase of vulnerability and decrease in firmness of functions of safety of the automated systems of higher education institution

On the basis of an integrated approach the main reasons for increase of vulnerability and decrease in firmness of functions of safety of the automated systems of a higher educational institution are considered. The analysis of consequences of automation of processes of safety and the related changes of system «protection system object of protection» is provided.

Keywords: the automated system, information security, object of protection, information security.
