УДК 681.32

КЛАССИФИКАЦИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

к.т.н. А.Ю. Гуль, И.Ю. Гуль, к.т.н. С.И. Марченко
(представил д.т.н., проф. Ю.И. Лосев)

В статье рассмотрены вопросы защиты конфиденциальной информации, приведена классификация угроз информационной безопасности автоматизированных систем, определены источники угроз безопасности информации, предложены пути повышения информационной безопасности и подходы для получения показателей защищенности информационных систем

Введение. Современные автоматизированные системы (АС) являются одним из краеугольных камней, на основе которых строят бизнес-процессы компании и предприятия различных форм и назначений. В то же самое время повышение значимости АС в бизнес-процессах предприятий, занятых производством товаров и услуг, обострило и проблемы защиты информационных ресурсов.

Говоря о защите информации, вводят следующую классификацию тайн по шести категориям: государственная тайна, коммерческая тайна, банковская тайна, профессиональная тайна, служебная тайна, персональные данные. Последние пять составляют конфиденциальную информацию.

Анализ литературы. Информация давно перестала быть просто необходимым для производства вспомогательным ресурсом или побочным проявлением всякого рода деятельности. Она приобрела ощутимый стоимостный вес, который четко определяется реальной прибылью, получаемой при ее использовании, или размерами ущерба, с разной степенью вероятности наносимого владельцу информации. Однако создание индустрии переработки информации порождает целый ряд сложных проблем. Одной из таких проблем является надежное обеспечение сохранности и установленного статуса информации, циркулирующей и обрабатываемой в информационно-вычислительных системах и сетях.

Цель статьи. Данная проблема вошла в обиход под названием проблемы защиты информации. Знание возможных угроз, а также уязвимых мест защиты, которые эти угрозы обычно эксплуатируют, необходимо для того, чтобы выбирать наиболее рациональные с экономической точки зрения средства обеспечения безопасности.

Анализ источников угроз. Считается, что безопасная система должна обладать устойчивостью к воздействиям, направленным на нарушение одной из трех характеристик информации, передаваемой, обрабатываемой или хранимой в АС, а именно – конфиденциальности, целостности или доступности.

Под конфиденциальностью (confidentiality) информации понимается свойство, позволяющее отказывать в праве на доступ к информации или не раскрывать ее неполномочным лицам, логическим объектам или процессам. Целостность (integrity) информации подразумевает ее способность не подвергаться изменению или аннулированию в результате несанкционированного доступа. И, наконец, доступность (availability) информации определяется, как свойство быть доступным и используемым по запросу со стороны уполномоченного пользователя [1].

Потенциальное действие, которое направлено на нарушение конфиденциальности, целостности и доступности информации, называется угрозой. Реализованная угроза называется атакой. Угроз безопасности не так уж много [2]:

- хищение (копирование) информации;
- уничтожение информации;
- модификация (искажение) информации;
- нарушение доступности (блокирование) информации;
- отрицание подлинности информации;
- навязывание ложной информации.

Носителями угроз безопасности являются источники угроз. В качестве источников угроз могут выступать как субъекты (личность), так и объективные проявления. Все источники угроз безопасности можно разделить на три основные группы [3]:

1) антропогенные источники угроз (обусловленные действиями субъекта);

2) техногенные источники угроз (обусловленные техническими средствами);

3) стихийные источники угроз.

Антропогенными источниками угроз безопасности выступают субъекты, действия которых могут быть квалифицированы как умышленные или случайные преступления. Только в этом случае можно говорить о причинении ущерба. Эта группа наиболее обширна и представляет наибольший интерес с точки зрения организации защиты, так как действия субъекта всегда можно оценить, спрогнозировать и принять адекватные меры. Методы противодействия в этом случае управляемы и напрямую зависят от воли организаторов защиты.

В качестве антропогенного источника угроз можно рассматривать субъекта, имеющего доступ (санкционированный или несанкционированный) к работе со штатными средствами защищаемого объекта. Субъекты (источники), действия которых могут привести к нарушению безопасности информации, могут быть как внешние, так и внутренние.

Внешние источники могут быть случайными или преднамеренными и иметь разный уровень квалификации [4]. К ним относятся:

– криминальные структуры;
– потенциальные преступники и хакеры;
– недобросовестные партнеры;
– технический персонал поставщиков телематических услуг;
– представители надзорных организаций и аварийных служб;
– представители силовых структур.

Внутренние субъекты (источники), как правило, представляют собой высококвалифицированных специалистов в области разработки и эксплуатации программного обеспечения и технических средств, знакомы со спецификой решаемых задач, структурой и основными функциями и принципами работы программно-аппаратных средств защиты информации, имеют возможность использования штатного оборудования и технических средств сети. К ним относятся:

– основной персонал (пользователи, программисты, разработчики);
– представители службы защиты информации;
– вспомогательный персонал (уборщики, охрана);
– технический персонал (жизнеобеспечение, эксплуатация).

Необходимо отметить, что специалисты по безопасности продолжают считать своих сотрудников и других лиц, имеющих доступ к внутренней информации; наиболее опасными с точки зрения угрозы безопасности для их организаций. Это является главной причиной, по которой они осуществляют мониторинг сотрудников.

К наиболее распространенным методам наблюдений относятся [5]:

– мониторинг соединений по Интернет (74%);
– изучение всего, что непосредственно связано с работой (62%);
– хранение и просмотр сообщений электронной почты (43%).
– запись сотрудников на работе на видеокамеры (18%);
– прослушивание телефонных разговоров сотрудников (12%);
– прослушивание сообщений голосовой почты сотрудников (7%).

Особую группу внутренних антропогенных источников составляют лица с нарушенной психикой и специально внедренные агенты. Данная группа рассматривается в составе перечисленных выше источников угроз, но методы парирования угроз этой группы могут иметь свои отличия.

Вторая группа содержит источники угроз, определяемые технократической деятельностью человека и развитием цивилизации. Этот класс источников угроз менее прогнозируемый, напрямую зависит от свойств технических средств и поэтому требует особого внимания.

Технические средства, являющиеся источниками потенциальных угроз безопасности также могут быть внешними:

– средства связи,
– сети инженерных коммуникаций (водоснабжения, канализации),
– транспорт;

и внутренними:

– некачественные технические средства обработки информации,
– некачественные программные средства обработки информации,
– вспомогательные средства (охраны, сигнализации, телефонии),
– другие технические средства, применяемые в организации.

Третья группа источников угроз объединяет, обстоятельства, составляющие непреодолимую силу, то есть такие обстоятельства, которые носят объективный и абсолютный характер, распространяющийся на всех. К непреодолимой силе в законодательстве и договорной практике относят стихийные бедствия или иные обстоятельства, которые невозможно предусмотреть или предотвратить или возможно предусмотреть, но невозможно предотвратить при современном уровне человеческого знания и возможностей. Такие источники угроз совершенно не поддаются прогнозированию и поэтому меры защиты от них должны применяться всегда.

Стихийные источники потенциальных угроз, как правило, являются внешними по отношению к защищаемому объекту и под ними понимаются, прежде всего, природные катаклизмы: (пожары, землетрясения, наводнения, ураганы. магнитные бури, радиоактивное излучение, различные непредвиденные обстоятельства, необъяснимые явления, другие форс-мажорные обстоятельства).

По данным исследований Института компьютерной безопасности США в последние три года наметилась тенденция к снижению потерь от различного рода атак [5 – 7] (табл. 1). Однако общее количество атак в процентном соотношении увеличивается [8], что отображено в табл. 2.

Ежегодному увеличению числа информационных атак на ресурсы АС способствуют следующие факторы [8]:

– увеличение количества уязвимостей, регулярно обнаруживаемых в существующем программно-аппаратном обеспечении АС;
– увеличение числа возможных объектов для атаки;
– упрощение интерфейсов программных средств реализации информационных атак;

– увеличение количества пользователей общедоступных сетей связи;

– недостаточное внимание, которое уделяется вопросам информационной безопасности.

Таблица 1

Общие потери от источников угроз по годам, долларов США

Источники угроз	**2002**	**2003**	**2004**
Telecom Eavesdropping (прослушивание)	346000	781000	0
Sabotage (вредительство)	15134000	5148500	871000
System Penetration (проникновение в систему)	13055000	2754400	901500
Web Site Defacement (уничтожение web-сайтов)	0	0	958100
Misuse of public Web Application (злоупотребления интернет-приложениями)	0	0	2747000
Telecom Fraud (мошенничества в сетях передач и данных)	6015000	701500	3997500
Unautorized Access by Insiders (несанкционированный доступ инсайдеров)	4503000	406300	4278205
Laptop/mobile theft (кражи с использованием беспроводной связи)	11766500	6830500	6734500
Financial Fraud (финансовые мошенничества)	115753000	10186400	7670500
Abuse of wireless network (нарушение работы беспроводных сетей)	0	0	10159250
Insider Abuse of Net Access (злоупотребление сетевыми ресурсами)	50099000	11767200	10601055
Theft of Proprietary Info (кража корпоративной информации)	170827000	70195900	11460000
DoS (отказ обслуживания)	18370500	65643300	26064050
Virus (Вирусная атака)	49979000	27382340	55053900
ВСЕГО	455848000	201797340	141496560

Таблица 2

Количество атак, % от числа опрошенных

Год	**Количество атак, %**			
	1 – 5	5 – 10	> 10	Не знаю
2000	33	23	13	31
2001	33	24	11	32
2002	42	20	15	23
2003	38	20	16	26
2004	47	20	12	21

Расчет показателей защищенности информационных систем. При анализе защищенности информационных систем необходимо оценивать усилия, затрачиваемые атакующим для преодоления средств защиты. Усилия иногда могут характеризоваться временем проникновения и преодоления защиты. Однако в более общем случае усилия представляют собой целое семейство параметров или их комбинации, включая финансовые расходы, время, опыт атакующего, количество вычислительных операций, необходимое для преодоления защиты и т.п. Использование усилия в качестве параметра защиты позволяет анализировать те ситуации, для которых параметр время не имеет смысла.

Примером такой ситуации является попытка проникновения в систему при помощи подкупа администратора или привилегированного пользователя, где удачность попытки полностью зависит от величины взятки (усилия).

Кроме оценки усилий, в [9] предлагается оценивать последствия этих усилий при помощи такого параметра, как вознаграждение атакующего. Вознаграждение, которое получит атакующий при проникновении в систему, определяет его мотивацию и его готовность затратить определенные усилия, необходимые для успешной атаки и проникновения. Примерами вознаграждения являются собственное удовлетворение, получение денег, любопытство.

Характеристики защиты должны рассматриваться не только с точки зрения атакующего, но и с точки зрения владельца системы или ее пользователей. С их точки зрения можно рассмотреть потери, которые возникают при проникновении в систему. Потери владельца являются некоторой функцией вознаграждений атакующего. На усилия атакующего также влияют затраты владельца на средства защиты. Чем больше затраты на средства защиты, тем большие усилия необходимы для их преодоления.

Таким образом, основой для получения показателей защищенности информационных систем могут служить вышеперечисленные четыре характеристики.

Выводы. Статистические данные показывают, что на практике редко применяется комплексный подход к вопросам информационной безопасности. Так, на предприятии могут быть установлены антивирусная программа и контроль доступа, но при этом слабо развиты программы обучения и информирования сотрудников, призванные помочь им эффективно использовать эти инструменты, и лишь в ограниченном объеме применяются процедуры тестирования систем, призванные обеспечить соблюдение норм законодательства.

В результате этого компании, стремясь обеспечить безопасность, могут возлагать неоправданные надежды на малоэффективные меры. Реализация надежной системы информационной безопасности возможна только при тщательном учете всех аспектов, включающих:

– комплексное понимание процесса обеспечения информационной безопасности;
– определение круга угроз системы информационной безопасности;
– определения набора возможных мер противодействия угрозам.

ЛИТЕРАТУРА

1. *Эрик С. Реймонд. Новый словарь хакера. – М., 1996. – 262 с.*
2. *Вакка Дж. Безопасность интранет. – М.,1998. – 496 с.*
3. *Вихорев С.В. Классификация угроз информационной безопасности. – [Электр. ресурс]. – Режим доступа: http://www.elvis.ru/files/class.pdf.*
4. *Петров А.А. Компьютерная безопасность. Криптографические методы защиты. – М., 2000. – 448 с.*
5. *2004 CSI/FBI Computer Crime and Security Survey Continue but Financial Losses are Down. Электр. ресурс]. – Режим доступа: http://i.cmpnet.com/ gocsi/db_area/pdfs/fbi/FBI2004.pdf.*
6. *2003 CSI/FBI Computer Crime and Security Survey Continue but Financial Losses are Down. Электр. ресурс]. – Режим доступа: http://i.cmpnet.com/ gocsi/db_area/pdfs/fbi/FBI2003.pdf.*
7. *2002 CSI/FBI Computer Crime and Security Survey Continue but Financial Losses are Down. Электр. ресурс]. – Режим доступа: http://i.cmpnet.com/ gocsi/db_area/pdfs/fbi/FBI2002.pdf.*
8. *Внутренние ИТ-угрозы в России 2004. Всероссийское исследование компании InfoWatch в области корпоративной защиты от внутренних угроз информационной безопасности. Электр. ресурс]. – Режим доступа: http://www.infowatch.ru/ downloads/docs/report2004.pdf.*
9. *Уткин Л.В., Шубинский И.Б. Нетрадиционные методы оценки надежности информационных систем. – СПб.: Любавич, 2000. – 540 с.*

Поступила 17.11.2004

ГУЛЬ Александр Юрьевич, *кандидат технических наук, начальник НИЛ ХУ ПС. Область научных интересов – кибернетика, теория графов, системы управления.*

ГУЛЬ Игорь Юрьевич, *начальник отдела информационных технологий торгово-промышленного холдинга "Идальго". Область научных интересов – автоматизированные системы управления, безопасность информации.*

МАРЧЕНКО Сергей Иванович*, кандидат технических наук, начальник кафедры ХУ ПС. Область научных интересов – кибернетика, автоматизированные системы управления, системы передачи данных, телекоммуникации.*