Глава II. Угрозы безопасности автоматизированным информационным системам (АИС)

2.1. Классификация угроз

Роль информации в жизни общества черезвычайно высока. Адекватное поведение каждого члена общества возможно только при наличии полной и достоверной информации о среде его деятельности и предмете его устремлений, при одновременном обеспечении конфиденциальности информации, находящейся в его распоряжении. Соответственно, и выполнение возложенных на АИС функций возможно при соблюдении подобных условий.

Событие, которое может вызвать нарушение функционирования АИС, включая искажение, уничтожение или несанкционированное использование обрабатываемой в ней информации, называется ***угрозой***. Возможность реализации угроз в АИС зависит от наличия в ней уязвимых мест. Состав и специфика уязвимых мест определяется видом решаемых задач, характером обрабатываемой информации, аппаратно-программными особенностями системы, наличием средств защиты и их характеристиками.

Совокупность угроз безопасности рассматривалась разными авторами во многих работах [35,36,54,30,152,58,100,16,122,73,30,186,146 и др.]. Основываясь на имеющемся опыте функционирования АИС, а также анализе результатов научных исследований [38,73,117,2] и практических разработок [186,130,6,32,128,26,95,103,8,67 и др.], следует выделить два типа угроз:

- *непреднамеренные или случайные действия*, выражающиеся в неадекватной поддержке механизмов защиты и ошибками в управлении;

- *преднамеренные угрозы* - несанкционированное получение информации и несанкционированная манипуляция данными, ресурсами и самими системами.

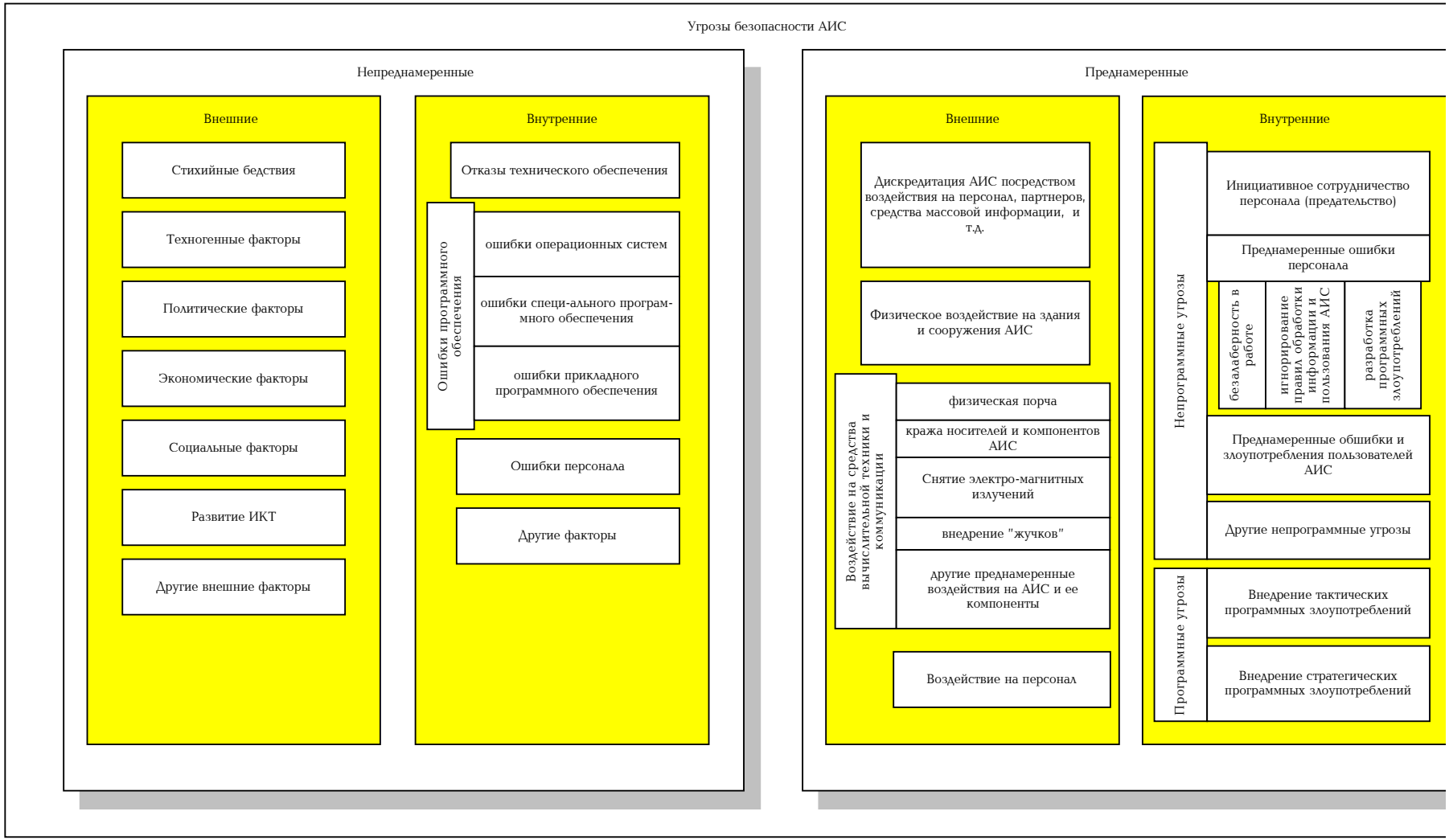

Рис.9. *Классификация угроз информационной безопасности АИС*

Выделение двух типов угроз является недостаточным и требует детализации. Классификация угроз безопасности АИС приведена на рис. 9 и включает разбиение с учетом внутренних и внешних факторов.

Множество непреднамеренных угроз, связанных с внешними (по отношению к АИС) факторами, обусловлено влиянием воздействий неподдающихся предсказанию. К ним относят угрозы, связанные с стихийными бедствиями, техногенными, политическими, экономическими, социальными факторами, развитием информационных и коммуникационных технологий, другими внешними воздействиями.

К внутренним непреднамеренным относят угрозы, связанные с отказами вычислительной и коммуникационной техники, ошибками программного обеспечения, персонала, другими внутренними непреднамеренными воздействиями, которые могут быть источниками угроз нормальной работы АИС.

Проблемы обеспечения надежности функционирования технических средств и программного обеспечения постоянно находились в центре внимания специалистов. В частности, вопросы отказоустойчивости вычислительной техники детально рассмотрены в работах [150,42,96], где исследуются виды ошибок, причины их возникновения, способы обнаружения, а также вопросы тестирования и т.д.

Вопросы надежности и отказоустойчивости программного обеспечения, рассмотренные в работах [96,33], связаны с логическими ошибками в постановке задач (например, несовершенство самого проекта), а также неправильной кодировкой, эксплуатацией и другими факторами. Как отмечено в [33], отдельную группу формируют непреднамеренные ошибки персонала при эксплуатации технических средств и программного обеспечения, что в свою очередь влияет на информационную безопасность. Непреднамеренные ошибки персонала обусловлены следующими группами факторов:

- недостаточной профессиональной подготовкой;

- эргономическими факторами;
- неправильной интерпретацией данных ввиду непонимания их специфики.

В рамках множества преднамеренных ошибок можно выделить угрозы, возникающие за пределами АИС и угрозы внутреннего характера. Следует отметить, что данное деление является условным, т.к. источник угроз может быть разным.

К распространенным преднамеренным информационным нарушениям относят [89,58,30 и др.]:

- несанкционированный доступ к информации, хранящейся в памяти компьютера и системы с целью несанкционированного использования;
- разработка специального программного обеспечения, используемого для осуществления несанкционированных доступа или других действий;
- отрицание действий, связанных с манипулированием информацией, и другие несанкционированные действия;
- ввод в программные продукты и проекты "логических бомб", которые срабатывают при выполнении определенных условий или по истечении опредeнного периода времени, частично или полностью выводят из строя компьютерную систему;
- разработка и распространение компьютерных вирусов;
- небрежность в разработке, поддержке и эксплуатации программного обеспечения, приводящие к краху компьютерной системы;
- изменение компьютерной информации и подделка электронных подписей;
- хищение информации с последующей маскировкой (например, использование идентификатора, не принадлежащего пользователю, для получения доступа к ресурсам системы);

- манипуляция данными (например, несанкционированная модификация, приводящая к нарушению целостности данных);
- перехват (например, нарушение конфиденциальности данных и сообщений);
- отрицание действий или услуги (отрицание существования утерянной информации);
- отказ в предоставлении услуги (комплекс нарушений, вызванных системными ошибками, несовместимостью компонент и ошибками в управлении).

Интересным является подход автора [87], который разделяет преднамеренные угрозы безопасности на:

- **физические**, к которым относят хищения, разбойные нападения, уничтожение собственности, террористические акции, другие черезвычайные обстоятельства;
- **технические**, к которым относят перехват информации, радиоразведку связи и управления, искажение информации, уничтожение информации, ввод ложной информации;
- **интеллектуальные** - уклонение от обязательств, мошенические операции, агентурная разведка, скрытое наблюдение, психологическое воздействие.

Под *несанкционированным доступом* (НСД) к ресурсам информационной системы понимаются действия по использованию, изменению и уничтожению исполняемых модулей и массивов данных системы, проводимые субъектом, не имеющим права на подобные действия [154].

Для получения доступа к ресурсам АИС злоумышленник обычно прибегает к следующим неправомерным действиям:

- отключение или видоизменение защитных механизмов;
- использование недоработок системы защиты для входа в систему;

- вход в систему под именем и с полномочиями реального пользователя.

В первом случае злоумышленник видоизменяеит защитные механизмы (например, отключает программу запроса паролей пользователей), во втором - изучает систему безопасности информации на предмет наличия недокументированных возможностей или недоработанных механизмов защиты и, в третьем - выясняет или с помощью определенных действий подделывает идентификатор реального пользователя (например, подсмотреть пароль, вводимый с клавиатуры).

При анализе источников угроз важно иметь в виду и различные разновидности нарушителей, которые могут быть систематизированы в следующие группы [62]:

- первая группа - так называемые хаккеры;

- вторая группа - преступники, преследующие цели обогащения путем непосредственного внедрения в финансовые системы или получения коммерческой и другой информации для организации действий уголовного характера;

- третья группа - террористы и другие экстремистские группы, использующие внедрение в информационные системы для совершения устрашающих действий, шантажа. Следует особо отметить, что с развитием компьютерных сетей INTERNET создается дополнительное киберпространство, в котором могут производится различные несанкционированные действия, и могут оставаться нераскрытыми;

- четвертая группа - различные коммерческие организации и структуры, стремящиеся вести промышленный шпионаж и борьбу с конкурентами путем добычи или искажения конфиденциальной финансовой, технологической, проектной, рекламной и другой информации.

Важно учитывать также и тот факт, что специфика рыночных отношений способствует использование более изощренных методов скрытого проникновения в файлы данных конкурирующих фирм.

Во всех случаях НСД может быть представлен как “своеобразную” модель опосредованного доступа. При этом проникновение в систему осуществляется на основе некоторого действия, реализованного пользователем или предварительно внедренной в систему программой либо несколькими программами.

По мере развития комплекса программно-технического, технологического, организационного и правового обеспечения совершенствовалась и концепция информационной безопасности. Одновременно развивались и средства для реализации НСД и других нежелательных действий.

Рассматривая комплекс программных злоупотреблений, которые получили распространение на сегодняшний день и исследованы в различных публикациях, необходимо отметить, что в отечественной и зарубежной литературе, посвященной проблеме безопасности АИС, преднамеренные воздействия рассматриваются с различных точек зрения и используются различные категории.

С.Мафтик при рассмотрении механизмов защиты в сетях ЭВМ выделяет только программы типа “троянский конь” [100]. В свою очередь, С.Недков, использует термин “программы проникновения в вычислительные системы” [107].

С появлением компьютерных вирусов получила распространение новая классификация компьютерных злоупотреблений. Н.Н. Безруков в [16, 18 и др.] рассматривает предшественников компьютерных вирусов - программы вандалы и троянские кони, с выделением в составе последних логических мин (logic bomb), мин с часовым механизмом (time bomb) и программных люков (trap doors).

В С.П.Расторгуев, использует термин ”средства скрытого информационного воздействия (ССИВ)”, понимая под ними вирусы и программные закладки [122]. В [73] предложен термин “разрушающие программные средства” (РПС), под которыми понимаются программно-реализуемые средства нарушения целостности обработки и хранения

информации в компьютерных системах. При этом выделяются три класса: компьютерные вирусы; средства несанкционированного доступа; программные закладки.

Авторы [6], описывая комплекс защиты для АИС с использованием баз данных, в качестве средств несанкционированного доступа выделяют специально разработанное программное обеспечение - ***программы - шпионы***.

Таким образом, в литературе уделяется внимание только узкому кругу программных злоупотреблений, оставляя за рамками исследований другие виды злоупотреблений, которые непосредственно связаны с АИС коммерческого назначения.

Авторами данной работы рассматривается термин “программные злоупотребления”, который наиболее полно с содержательной и функциональной точки зрания отражает природу подобного вида угроз [186].

Интересным является подход к классификации угроз безопасности АИС, представленный в [14] и предусматривающий их систематизацию по следующим основным признакам на следующие их разновидности:

а) по признаку области поражения: угрозы для информационной среды, ее подсистем и элементов; угрозы для предметных областей информационного обеспечения - субъектов и объектов пользования; угрозы для всей социальной системы, исходящие от информационной среды;

б) по признаку их связи с информационной средой определенной социальной системы: внешние; внутренние, идущие от социальной системы и ее элементов; внутрисистемные - исходящие от самой информационной среды;

в) по силе воздействия на область поражения выделяются: разрушительные; дестабилизирующие; парализующие и стимулирующие угрозы;

г) по организационной форме выражения и степени социальной опасности: коллизии, конфликты, проступки, преступления, аварии и катастрофы.

Рассмотренная система классификации угроз реализована с точки зрения информационной безопасности общества и информационных процессов, происходящих в нем. Следует отметить ее функциональную наполненность и емкость.

Наиболее полная классификация угроз безопасности АИС представлена в [30]. Авторы монографии предлагают выделение разновидностей по следующим признакам:

- по цели реализации угрозы: нарушение конфиденциальности, нарушение целостности, нарушение доступности;

- по принципу воздействия: с использованием доступа, с использование скрытых каналов;

- по характеру воздейтсвия: активные, пассивные;

- по причине появления используемой ошибки защиты: неадекватность политики безопасности, ошибки управления системой защиты, ошибки проектирования системы защиты, ошибки кодирования;

- по способу воздействия на объект атаки: непосредственное воздействие на объект атаки, воздействие на систему разрешений, опосредованное воздействие;

- по способу воздействия: в интерактивном и пакетном режимах;

- по объекту атаки: на АИС в целом, на объекты АИС, на субъекты АИС, на каналы передачи данных;

- по используемым средствам атаки: с использованием штатного программного обеспечения, с использованием разработанного программного обеспечения;

- по состоянию объекта атаки: при хранении объекта, при передаче объекта, при обработке объекта.

Таким образом, в настоящее время отсутствует единый подход к классификации программных злоупотреблений (ПЗ), поскольку они лишь недавно стали объектом пристального внимания и исследования. Кроме того, многообразие форм проявлений, различия во внутренней организации, жизненный цикл и среда обитания - все это существенно усложняет создание единого классификатора. В среде пользователей персональных ЭВМ получила распространение неформальная классификация, в соответствии с которой большинство ПЗ определяется как компьютерные вирусы и им присваивают наименование предполагаемого места разработки или обнаружения, либо число, характеризующее длину вирусного механизма [17].

В компьютерной среде появление вирусов связывается с взаимодействием трех направлений совершенствования элементов ИТ [16]:

- разработка самовоспроизводящихся программ;

- создание программ для повреждения или уничтожения других программ;

- освоение массового производства персональных компьютеров.

Нам представляется необходимым дополнить рассмотренные подходы к классификации угроз безопасности АИС концентрируя внимание на преднамеренных угрозах - программных злоупотреблениях. Считаем возможным предложить новую классификацию, приведенную на рис 10 и призванную дополнить и расширить предложенные в [30,14] классификации.

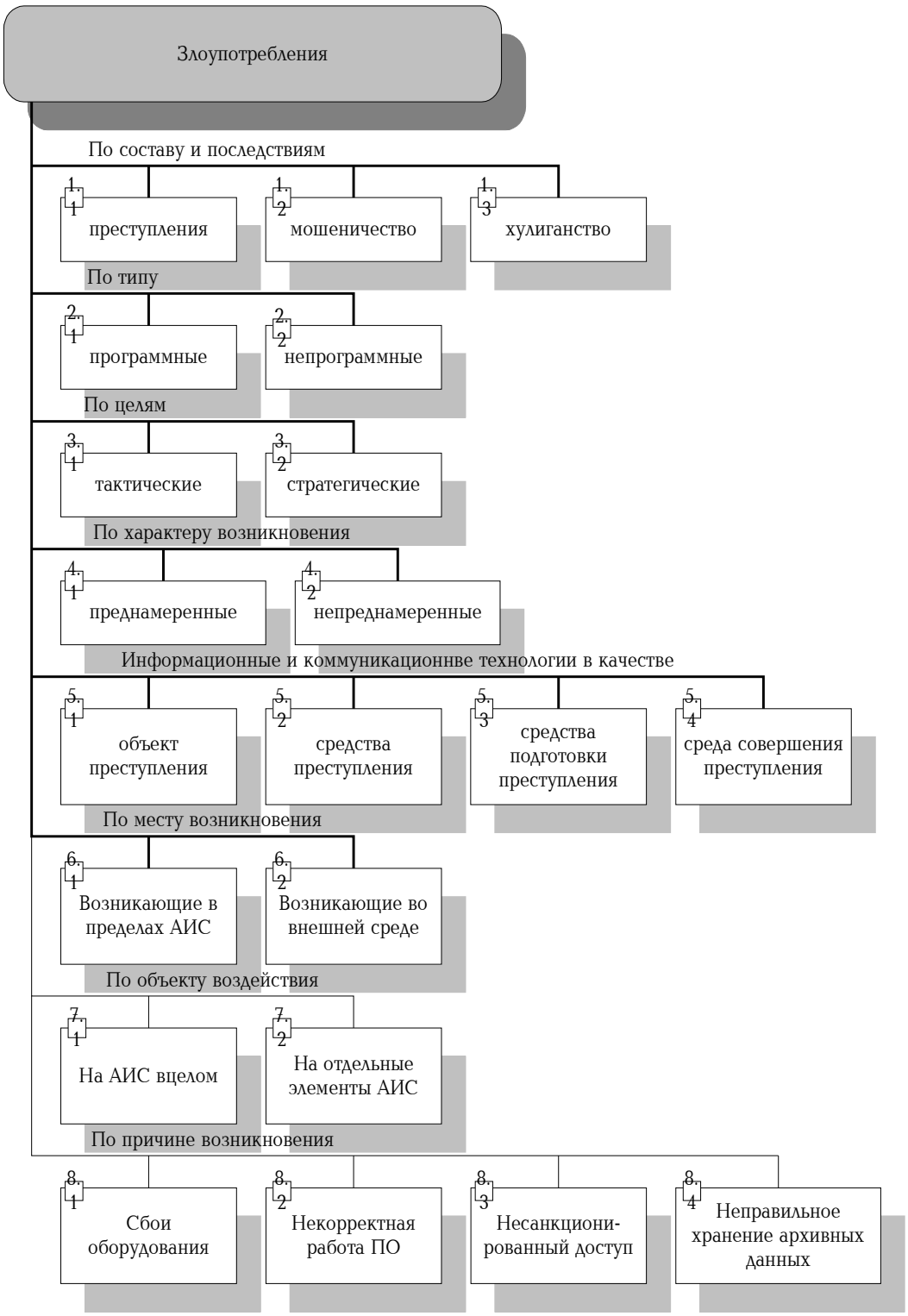

Рис. 10 Классификация уроз информационной безопасности АИС.

Как видно из рис. 10, по составу и последствиям ПЗ представляются в виде *преступлений*, *мошеничеств и хулиганств*. В последнее время широкое распространение получила также разновидность компьютерных преступлений как компьютерное мошенничество и хулиганство.

Компьютерное мошенничество отличается от других видов компьютерных нарушений тем, что что его целью является незаконное обогащение нарушителя.

Компьютерное хулиганство, на первый взгляд, является безобидной демонстрацией интеллектуальных способностей, но последствия подобных действий могут быть весьма серьезными, поскольку они приводят к потере доверия пользователей к вычислительной системе, а также к краже данных, характеризующих личную или коммерческую информацию.

Под компьютерным преступлением (КП) следует понимать комплекс противоправных действий, направленных на несанкционированный доступ, получение и распространение информации, осуществляемых с использованием средств вычислительной техники, коммуникаций и ПО.

Группа экспертов из Организации экономического сотрудническтва и развития в 1983 г. определила, что под термином ”компьютерная преступность” (или “связанная с компьютерами преступность”) трактуются любые незаконные, неэтичные или неправомерные действия, связанные с автоматической обработкой данных и/или их передачей [57]. В той же работе определены основные виды компьютерной преступности:

1) связанные с компьютерами экономические преступления, среди которых можно различать шесть основных видов:

- махинации путем компьютерного манипулирования АИС в целях получения финансовой выгоды;
- компьютерный шпионаж и кража программного обеспечения;
- компьютерные диверсии;

- кража услуг (времени), неправомерное использование АИС;

- неправомерный доступ к АИС и их “взламывание”;

- традиционные преступления в сфере бизнеса (экономики), совершаемые с помощью АИС.

2) нарушение личных прав. К такого вида нарушения можно отнести следующие действия:

- составление и использование некорректных данных;

- незаконное раскрытие данных или их использование не по назначению (данное действие частично входит в сферу традиционных преступлений, связанных с производственными секретами);

- незаконный сбор и хранение данных;

- нарушение формальных обязанностей и информационного права в соответствии с законами о частной тайне.

3) компьютерные преступления против “индивидуальных” интересов, таких, как преступления против национальной безопасности, трансграничного потока данных, неприкосновенности компьютерных процедур и сетей передачи данных и другие;

Следует отметить, что представленная классификация является условной и дальнейшее уточнение должно проводиться в рамках существующих правовых актов.

По типу реализации можно различать *программные* и *непрограммные* злоупотребления. К программным относят злоупотребления, которые реализованы в виде отдельного программного модуля или модуля в составе программного обеспечения. К непрограммным относят злоупотребления, в основе которых лежит использование технических средств АИС для подготовки и реализации компьютерных преступлений (например, несанкционированное подключение к коммуникационным сетям, съем информации с помощью специальной аппаратуры и др.)

Компьютерные злоумышленники преследуют различные цели и для их реализации используют широкий набор программных средств.

Исходя из этого, представляется возможным объединение программных злоупотреблений в две группы: *тактические и стратегические*. К тактическим относят злоупотребления, которые преследуют достижение ближайшей цели (например, получение пароля, уничтожение данных и др.). К группе стратегических относятся злоупотребления, реализация которых обеспечивает возможность получения контроля за технологическими операциями преобразования информации, влияние на функционирование компонентов АИС (например, мониторинг системы, вывод из строя аппаратной и программной среды и др.).

По характеру возникновения различают *непреднамеренные* и *преднамеренные* злоупотребления. Непреднамеренные угрозы связаны с стихийными бедствиями и другими неподдающимися предсказанию факторами, сбоями и ошибками вычислительной техники и программного обеспечения, а также ошибками персонала. Преднамеренные угрозы обусловлены действиями людей и ориентированы на несанкционированное нарушение конфиденциальности, целостности и/ или доступности информации, а также использование ресурсов в своих целях.

При реализации угроз безопасности информационные и коммуникационные технологии могут выступать в качестве объекта преступления, средства преступления, средства подготовки преступления или среды совершения преступления [89].

По месту возникновения угроз безопасности АИС можно различать угрозы,возникающие в пределах АИС и угрозы, возникающие во внешней среде.

По объекту воздействия следует выделять угрозы, воздействующие на АИС в целом и угрозы, воздействующие на отдельные ее элементы.

По причине возникновения различают такие угрозы, как сбои оборудования, некорректная работа операционных систем и программного обеспечения, несанкционированный доступ и

неправильное хранение архивных данных, вследствии чего они могут быть утеряны (уничтожены).

Несанкционированные манипуляции с информацией и ресурсами АИС могут приводить к следуюшим разновидностям их последствий:

- *утрата информации* - неосторожные действия владельца информации, представленной в АИС на различных носителях и в файлах, или лица, которому была доверена информация в силу его официальных обязаностей в рамках АИС, в результате которых информация была потеряна и стала достоянием посторонних лиц;

- *раскрытие информации* - умышленные или неосторожные действия, в результате которых содержание информации, представленной на различных носителях и в файлах, стало известным или доступным для посторонних лиц;

- *порча информации* - умышленные или неосторожные действия, приводящие к полному или частичному уничтожению информации, представленной на различных носителях и в файлах;

- *кража информации* - умышленные действия, направленные на несанкционированное изъятие информации из системы ее обработки как посредством кражи носителей информации, так и посредством дублирования информации, представленной в виде файлов АИС;

- *подделка информации* - умышленные или неосторожные действия, в результате которых нарушается целостность информации, находящейся на различных носителях и в файлах АИС;

- *блокирование информации* - умышленные или неосторожные действия, приводящие к недоступности информации в системе ее обработки;

- *нарушение работы системы обработки информации* - умышленные или неосторожные действия, приводящие к частичному или полному отказу системы обработки или создающие благоприятные условия для выполнения вышеперечисленных действий.

В таблице 1 представлены основные группы несанкционированных действий, нарушающих безопасность информации.

Таблица 1

Несанкционированные действия по отношению к ресурсам АИС и нарушенные свойства безопасности

	Нарушение конфиденциальности	Нарушение целостности	Нарушение доступности
Утрата информации	+	+	+
Раскрытие информации	+	-	-
Порча информации	-	+	+
Кража информации	+	-	+
Подделка информации	-	+	-
Блокирование информации	-	-	+
Нарушение работы АИС	-	-	+

Реализация нарушителями угроз безопасности АИС приводит к нарушению нормального функционирования АИС и/или к снижению безопасности информации, определенное конфиденциальностью, целостностью и доступностью.

Исходя из вышеизложенного необходимо разрабатывать методы и средства обеспечения информационнйо безопасности АИС.