имеет период $l = (2^{19937} - 1)/32 \approx 1{,}3486 \cdot 10^{6000}$, который многократно превосходит значение A и удовлетворяет приведённому неравенству. Вышесказанное доказывает, что при использовании ГПСЧ «Вихрь Мерсенна» возможно с помощью лишь одной функции получить необходимое количество последовательностей для повышения структурной скрытности НС в течение 15 лет. При этом выбор начального бита ГПСЧ в качестве секрета позволит обеспечить высокую структурную скрытность кодовых последовательностей.

Проведённый вычислительный эксперимент по моделированию систем квазиортогональных кодовых последовательностей на основе разработанного метода позволяет получать системы кодовых последовательностей, удовлетворяющих корреляционным и статистическим требованиям и имеющих высокую сложность разгадывания структуры [7].

Таким образом, повысить помехозащищённость интерфейса потребителей ГНСС предлагается путём повышения структурной скрытности НС ГНСС на основе стохастического использования систем квазиортогональных кодовых последовательностей. Для этого был разработан метод моделирования увеличенного количества систем двоичных квазиортогональных кодовых последовательностей с высокой сложностью разгадывания структуры.

Литература

1. Орёл Д. В. Анализ угроз функционирования аппаратуры гражданских потребителей глобальных спутниковых радионавигационных систем // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. Ростов-н/Д.: ПЦ «Университет» СКФ МТУСИ, 2011. С. 44–48.

2. Дятлов А. П., Дятлов П. А., Кульбикаян Б. Х. Радиоэлектронная борьба со спутниковыми радионавигационными системами. М.: Радио и связь, 2004. 226 с.

3. Общесистемные вопросы защиты информации: коллективная монография / под ред. Е. М. Сухарева. Кн. 1. М.: Радиотехника, 2003. 296 с.

4. Вентцель Е. С. Теория вероятностей. 4-е изд., стереотип. М.: Наука, 1969. 576 с.

5. Вадзинский Р. Н. Справочник по вероятностным распределениям. СПб.: Наука, 2001. 295 с.

6. Ипатов В. П. Периодические дискретные сигналы с оптимальными корреляционными свойствами. М.: Радио и связь, 1992. 152 с.

7. Жук А. П., Орёл Д. В. Моделирование кодовых последовательностей для сигналов глобальных спутниковых радионавигационных систем с кодовым разделением каналов // Материалы XVI Международной научно-технической конференции «Радиолокация. Навигация. Связь». Воронеж: НПФ «Саквоее», 2010. С. 2111–2119.

УДК 004.942

Росенко Александр Петрович, Окулова Мария Сергеевна

АНАЛИЗ И ОБОБЩЕНИЕ СУЩЕСТВУЮЩИХ ПОДХОДОВ К КЛАССИФИКАЦИИ УГРОЗ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

В статье авторами осуществляется анализ угроз безопасности конфиденциальной информации по различным классификационным признакам; авторы на основе анализа и обобщения имеющихся данных представили информацию о существующих подходах к классификации угроз безопасности конфиденциальной информации.

Ключевые слова: внутренние угрозы, конфиденциальная информация, ущерб.

Rosenko Alexander Petrovitch, Okulova Maria Sergeevna

THE ANALYSIS AND GENERALIZATION AVAILABLE APPROACHES OF CLASSIFICATION OF THREATS FOR PRIVATE DATA'S SAFETY

In article authors the analysis of threats for private data's safety on various classification signs is carried out. Authors of this article the analysis and generalization of existing information, submitted information about available approaches of classification of threats for private data's safety.

Key words: insider's threats, private data, detriment, insiders.

Обеспечение безопасности конфиденциальной информации всегда было одной из важнейших проблем теории защиты информации (ЗИ). Утечка конфиденциальной информации, интеллектуальной собственности, информации ноу-хау является следствием значительного материального и морального

ущерба, который наносится не только собственнику информации ограниченного распространения, но и государству в целом. Это связано с очевидными и вполне объективными закономерностями, которые проявляются в современных непростых условиях информационных взаимоотношений.

Актуальность проблемы разделения угроз по отдельным классификационным параметрам стала очевидной в процессе развития компьютерных систем, широкого применения автоматизированных систем сбора и обработки данных, в которых циркулируют массивы конфиденциальной информации (КИ), утечка или утеря которых может привести к существенному, а порой и непоправимому ущербу собственнику информации.

Исследования показывают [1–5], что в настоящее время универсальной классификации угроз безопасности КИ не существует. Это связано с тем, что практически постоянно осуществляется разработка и внедрение новых методов и средств незаконного воздействия злоумышленника на КИ, появляются новые более совершенные вирусы, используются возможности по внедрению различных программных закладок злоумышленником.

Обеспечение безопасности КИ невозможно без систематической постоянной работы по анализу возможных негативных последствий для собственника КИ, связанных с воздействием на КИ различного рода угроз, их анализу, систематизации, основе которых следует дальнейшая разработка действенных и своевременных мероприятий по обеспечению сохранности КИ.

В то же время действенность таких мероприятий обусловливается необходимостью идентификации возможных источников угроз, факторов, способствующих их проявлению. В конечном итоге эффективность такой работы определяется наличием системной классификации угроз безопасности КИ.

В настоящее время созданы различные подходы к классификации угроз безопасности КИ. При этом различные авторы по своему трактуют не только само понятие «угрозы», но и вкладывают различный смысл в понятие классификационных признаков, а также в структуру построения самой классификации [1–7]. Рассмотрим основные заслуживающие интереса подходы к классификации угроз безопасности КИ различных авторов, их структуру, содержание, достоинства и недостатки.

В основу классификации специалистами фирмы Digital Security положен алгоритм оценки рисков с учетом анализа угроз и уязвимостей информационных систем. Специалисты фирмы Digital Security предложили следующую классификацию угроз безопасности информации, наиболее полно, по их мнению, отвечающую анализу рисков реальных информационных систем:

1) технологические;

2) организационные.

Технологические угрозы подразделяются на физические и программные.

В последующем при рассмотрении классификации технологических угроз показано, что физические угрозы, в свою очередь, могут исходить от действий человека, форс-мажорных обстоятельств и отказа оборудования, а программные (логические) – от локального нарушителя и удаленного нарушителя. Далее предполагается, что если нарушитель имеет физический доступ к КИ, то он может воздействовать непосредственно на ресурс либо на канал связи.

Организационные угрозы КИ подразделяются следующим образом: воздействие на персонал (физическое и психологическое); действия персонала (умышленные или неумышленные).

Таким образом, классификация угроз DSECCT специалистами фирмы Digital Security включает в себя классификацию по виду, характеру воздействия, причине и объекту угрозы – в этом заключается преимущество данной классификации.

Однако такая классификация не отражает классификацию угроз по способам, методам реализации угроз, последствиям от реализации угроз для собственника КИ и другим важнейшим классификационным признакам, таким как зависимость или независимость угроз, время воздействия угроз на КИ и др. – в этом заключаются основные недостатки данной классификации.

Сотрудники [7] в основу классификации угроз безопасности информации положили в качестве основного элемента современной АИС систему управления базами данных (СУБД). Поэтому наряду с основными общими угрозами безопасности информации, такими как несанкционированный доступ к информации, программно-технические воздействия по каналам связи, утечка данных за счет побочных электромагнитных излучений и наводок в АИС, имеют место специфические угрозы прикладных баз данных (БД) за счет использования уязвимых мест СУБД.

По мнению указанных сотрудников, к специфическим угрозам можно отнести следующие: несанкционированное получение информации путем логических выводов; нарушение конфиденциальности информации путем агрегирования данных; снижение коэффициента готовности; внесение закладок в стандартные механизмы обеспечения безопасности или поддержания целостности данных; использование расширенных хранимых процедур СУБД в целях нарушения ИБ.

При этом авторы подчеркивают, что нарушение конфиденциальности информации путем агрегирования данных – это метод получения дополнительной информации, на доступ к которой нет полномочий путем комбинирования данных, добытых легальным образом из различных таблиц в обобщенную информацию.

Под снижением коэффициента готовности авторы понимают возможность при использовании нарушителем или некомпетентным пользователем длительных транзакций, захватывающих большое количество таблиц.

Внесение закладок в стандартные механизмы обеспечения безопасности или поддержания целостности данных авторы рассматривают как специфическую часть проблемы АИС, которая усугубляется сложностью контроля над правильностью написания хранимых процедур, ограничений, правил в СУБД.

Использование расширенных хранимых процедур СУБД для несанкционированного доступа к информации прикладной БД АИС является специфической угрозой обеспечения безопасности СУБД, имеющей двухуровневую архитектуру «клиент – сервер».

Авторы предлагают дополнить модели угроз прикладных баз данных указанными специфическими угрозами безопасности, что, по их мнению, позволит повысить защищенность прикладной БД современных СУБД.

Указанная классификация заслуживает внимания при анализе и построении политики безопасности СУБД. В то же время такая классификация не является всесторонней и не в полной мере охватывает все возможные угрозы безопасности КИ, воздействующие на АИС.

В работе [3] предложена классификация угроз безопасности информации, циркулирующей в корпоративной сети. Авторы придерживаются общепризнанной классификации, в соответствии с которой все источники угроз безопасности информации, циркулирующей в корпоративной сети, можно разделить на три основные группы: угрозы, обусловленные действиями субъекта (антропогенные угрозы); угрозы, обусловленные техническими средствами (техногенные угрозы); угрозы, обусловленные стихийными бедствиями.

В предложенной классификации достаточно подробно рассматриваются как внешние, так и внутренние субъекты, действия которых могут привести к нарушению безопасности информации, а также к возможным последствиям от таких действий.

Особенностью предложенной классификации является то, что авторы для обеспечения комплексной безопасности показали необходимость учета как организационных, так и технических решений парирования угроз.

Другой особенностью необходимо отметить стремление авторов на основе анализа статистической информации придать каждой угрозе весовые коэффициенты и таким образом классифицировать угрозы по частоте проявления угрозы безопасности информации.

В исследованиях [1, 2, 4, 5] авторы предложили классификацию внутренних угроз, которая, по их мнению, позволяет не только охватить все сценарии реализации внутренних угроз, но и систематизировать представленные на рынке средства защиты от таких угроз. Классификация внутренних угроз, предлагаемая авторами, выглядит следующим образом:

1) разглашение КИ;
2) обход средств защиты от разглашения КИ;
3) кража КИ;
4) нарушение авторских прав на информацию;
5) нецелевое использование ресурсов компании.

Как видно из представленного материала, предложенная классификация является ограниченной и не может носить системный характер.

Авторы работ [2, 4, 5] связывают классификацию угроз с таким понятием, как «ущерб». При этом проявления возможного ущерба, по мнению авторов, могут быть различны, а именно:

1) моральный и материальный ущерб репутации организации;

2) моральный, физический, материальный ущерб, связанный с разглашением персональных данных отдельных лиц;

3) материальный ущерб от разглашения КИ;

4) материальный ущерб от необходимости восстановления нарушенных защищаемых информационных ресурсов;

5) материальный ущерб от невозможности выполнения взятых на себя обязательств перед третьей стороной;

6) моральный и материальный ущерб от дезорганизации деятельности организации;

7) материальный и моральный ущерб от нарушения международных соглашений.

Ряд авторыов [2, 5] рассматривают понятие «угрозы» с точки зрения интересов субъектов информационных отношений, главным образом от того, какой ущерб для них является неприемлемым. В связи с этим угрозы, по мнению авторов, можно классифицировать по нескольким критериям:

1) по аспекту ИБ (доступность, целостность конфиденциальность), против которого угрозы направлены в первую очередь;

2) по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);

3) по способу осуществления (случайные, преднамеренные, техногенные и т. п.);

4) по расположению источника угроз (внутренние, внешние).

Некоторые авторы [3, 8] рассматривают возможность реализации угроз в зависимости от наличия в АИС уязвимых мест, количество и специфика которых определяется видом решаемых задач, характером обрабатываемой информации, аппаратно-программными особенностями системы, наличием средств защиты и их характеристиками. Основываясь на результатах научных исследований практических разработок, авторы выделяют два типа угроз:

1) непреднамеренные, или случайные действия, выражающиеся в неадекватной поддержке механизмов защиты и ошибками в управлении;

2) преднамеренные угрозы – несанкционированное получение информации и несанкционированная манипуляция данными, ресурсами, самими системами.

При этом к внутренним непреднамеренным угрозам авторы относят угрозы, связанные с отказами вычислительной и коммуникационной техники, ошибками программного обеспечения, персонала и другими воздействиями, которые могут быть источниками угроз штатной работе АИС.

В то же время некоторые авторы разделяют преднамеренные угрозы безопасности информации:

1) на физические, к которым относят хищение информации, разбойные нападения, уничтожение информации, террористические акции и т. п.;

2) технические, к которым относят перехват информации, радиоразведку связи и управления, искажение, уничтожение и ввод ложной информации;

3) интеллектуальные – уклонение от обязательств, мошеннические операции, агентурная разведка, скрытое наблюдение, психологическое воздействие.

Заслуживает внимания подход к классификации угроз безопасности КИ, представленный в работе [3]. Автор классифицирует угрозы следующим образом:

1) по признаку области поражения (например, угрозы для АИС, ее подсистем и элементов);

2) по признаку их связи с информационной средой (внешние, внутренние, внутрисистемные);

3) по силе воздействия на область поражения: разрушительные, дестабилизирующие, парализующие и стимулирующие угрозы;

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

Подобная классификация угроз безопасности КИ представлена и в статье [6], где авторы дополнили классификацию, предложенную в исследовании [9], в частности по таким параметрам, как используемые средства атаки, состояние объекта атаки и др.

Таким образом, представленный анализ свидетельствует о том, что в настоящее время отсутствует единый подход к классификации угроз безопасности КИ. Это связано с тем, что:

1) пристальное внимание к классификации угроз появилось сравнительно недавно;

2) многообразие угроз, форм их проявлений, внешние условия существенно усложняют создание единого классификатора;

3) при создании классификации внутренних угроз необходимо учитывать ряд основополагающих обстоятельств, которые диктуются целью, задачами, объектом исследования, необходимостью учета многочисленных факторов, проявляющихся в процессе функционирования АИС;

4) создание единой системной классификации по всем основным угрозам безопасности КИ в настоящее время затруднительно.

В то же время анализ показывает, что при создании классификации необходимо учитывать следующие общие рекомендации:

1) какие угрозы по виду рассматриваются (техногенные, антропогенные, стихийные бедствия);

2) какова цель создания классификации;

3) какие методики, математические модели разработаны для исследования угроз безопасности КИ;

4) какая априори имеется информация по частоте проявления различных угроз, степени их опасности для КИ, применяемые методы и средства парирования угроз.

Анализ и обобщение существующих подходов классификации угроз безопасности КИ показал, что в настоящее время универсальной классификации угроз безопасности КИ не существует. В статье были рассмотрены и проанализированы различные существующие классификации угроз. Было показано, что ни одна из проанализированных классификаций в полной мере не применима для описания большинства существующих угроз. Во многих случаях реальные угрозы либо не подходили ни под один из классификационных признаков, либо, наоборот, удовлетворяли нескольким.

Литература

1. Шатунов С. В., Батищев А. Г. Алгоритм определения уровня конфиденциальной информации в автоматизированных системах // Материалы V Международной научно-практической конференции «Информационная безопасность». Таганрог: Изд-во ТРТУ, 2003. С. 73–78.

2. Березовский С. В., Мецатунян М. В. Основные угрозы информационным ресурсам предприятия // Материалы V Международной научно-практической конференции «Информационная безопасность». Таганрог: Изд-во ТРТУ, 2003. С. 101–103.

3. Складчиков С. Е. Применение методов нечеткой логики в системах обнаружения атак // Научная сессия МИФИ-2002. IX Всероссийская научно-практическая конференция «Проблемы информационной безопасности в системе высшей школы»: сборник научных трудов. М.: Изд-во МИФИ, 2002. С. 102–104.

4. Финадорин Г. А. Использование теории случайных процессов для оценки безопасности полетов. К.: КВВАИУ, 1983. 180 с.

5. Мосолов А. С., Новиков Ю. В. Обобщенный критерий оценки эффективности подсистемы обнаружения СКБ и оценки вероятности обнаружения нарушителя // Материалы VI Международной научно-практической конференции «Информационная безопасность». Таганрог: Изд-во ТРТУ, 2004. С. 116–118.

6. Григорьева Т. В., Иванов С. М., Панфилов А. П., Язов Ю. К. Метод количественной оценки защищенности информации в компьютерной системе // Материалы IX Международной научно-практической конференции «Информационная безопасность». Таганрог: Изд-во ТТИ ЮФУ, 2007. Ч. 1. С. 151–156.

7. Запечников С. В. Проблемы оценки уровня защищенности информации в АСОД // Научная сессия МИФИ-2002. IX Всероссийская научно-практическая конференция «Проблемы информационной безопасности в системе высшей школы». Сборник научных трудов. М.: Изд-во МИФИ, 2002. С. 65–67.

8. Лаврентьев В. С., Толстой А. И., Харламов В. П. Безопасность и аудит базы данных с позиции администратора безопасности организации // Научная сессия МИФИ-2002. IX Всероссийская научно-практическая конференция «Проблемы информационной безопасности в системе высшей школы»: сборник научных трудов. М.: Изд-во МИФИ, 2002. С. 56–58.

9. Росенко А. П., Аветисов Р. С. Методика оценки величины ущерба от воздействия на автоматизированную информационную систему внутренних угроз // Известия ТРТУ. Тематический выпуск. Таганрог: Изд-во ТРТУ, 2006. С 33–37.