ТЕХНИЧЕСКИЕ НАУКИ

Смык Сергей Владимирович
канд. техн. наук, доцент
ФГАОУ ВО «Национальный исследовательский университет «Московский институт электронной техники»
г. Москва
Уварова Анна Игоревна
студент
ФГАОУ ВО «Национальный исследовательский университет «Московский институт электронной техники»
г. Москва
Рекунков Иван Сергеевич
канд. техн. наук, доцент
ФГБОУ ВО «Московский государственный университет информационных технологий, радиотехники и электроники»
г. Москва

АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ЭКСПЛУАТАЦИИ ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫХ СИСТЕМ

***Аннотация**: в данной статье рассмотрены актуальные угрозы безопасности информации при эксплуатации современных информационно-измерительных систем и средств измерений иностранного производства.*

***Ключевые слова**: угрозы безопасности информации, измерительная информация, информационно-измерительная система, несанкционированный доступ, специальное программно-техническое воздействие.*

Уровень развития современного государства, включая его промышленность, оборону, медицину, науку, строительство, торговлю, экологию, в значительной мере определяется состоянием метрологического обеспечения и парком средств измерений (СИ). Каждую секунду в нашей стране производятся

миллионы измерительных операций, результаты которых используются для обеспечения надлежащего качества и технического уровня выпускаемой продукции, обеспечения безопасности государства, безопасной и безаварийной работы транспорта, для установления медицинских и экологических заключений и других целей.

Большинство современных СИ, применяемые в науке и технике, в том или ином виде, представляют собой измерительные системы и измерительные комплексы, управляемые соответствующим программным обеспечением (ПО), представляющие собой информационно-измерительные системы (ИИС).

Под понятием «информационно-измерительные системы» понимают совокупность соединенных между собой СИ и других технических устройств, реализующих процесс измерений и обеспечивающих автоматическое (автоматизированное) получение информации об изменяющихся во времени и распределенных в пространстве физических величинах, характеризующих определенные свойства или состояния объекта измерений, а также обладающих возможностью хранения и передачи измерительной информации об объекте измерения.

Одним из ключевых факторов обеспечения единства измерений при эксплуатации такого рода ИИС является обеспечение достоверности измерительной информации. Получение достоверной измерительной информации возможно при выполнении множества условий, одним из таких условий является обеспечения защиты оборудования, ПО и результатов измерений от несанкционированного доступа (НСД) на физическом и программном уровне [2].

Несанкционированное воздействие на измерительную информацию в процессе эксплуатации ИИС различного назначения может осуществляться, с целью нарушения основных свойств этой информации. Решение задач, связанных с предотвращением такого рода воздействий на информацию, осуществляется в рамках реализации мероприятий по защите информации и обеспечения информационной безопасности.

Широкое использование в нашей стране СИ иностранного производства, реализующих, в том числе и, измерительные технологий при помощи системного

и прикладного ПО, неизбежно увеличивает риски несанкционированного воздействия на измерительную информацию. Оценка рисков, связанных с применением тех или иных СИ и измерительных технологий иностранного производства, в отраслях науки и технике нашего государства, невозможна без анализа актуальных угроз безопасности, обрабатываемой ими информации.

В соответствии с [1] основными свойствами информации являются: конфиденциальность (обеспечение правомерного – с разрешения обладателя информации – доступа к информации, распространения и предоставления её), целостность (обеспечение достоверности и полноты информации) и доступность (возможность получения информации и её использование).

В свою очередь под угрозой безопасности информации будем понимать совокупность условий и факторов (явлений, действий или процессов), создающих потенциальную или реально существующую опасность, в результате которой возможны утечка информации, неправомерное модифицирование (искажение, подмена), уничтожение информации или неправомерное блокирование доступа к ней [3].

Состав и содержание угроз безопасности измерительной информации определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к информации. Совокупность таких условий и факторов формируется с учетом характеристик ИИС, свойств среды распространения информативных сигналов, содержащих защищаемую измерительную информацию, и возможностей источников угрозы.

К характеристикам ИИС, обусловливающим возникновение угроз безопасности измерительной информации, можно отнести объем и вид обрабатываемых в ИИС данных, структуру ИИС, наличие подключений ИИС к локальным сетям, режимы работы ИИС, местонахождение и условия размещения элементов ИИС, а также страна разработчик (изготовитель) элементов ИИС.

Основными элементами ИИС (объектами зашиты информации) являются:

– измерительная информация, как совокупность информации и ее носителей, используемых в ИИС;

– информационные технологии, применяемые при обработке измерительной информации;

– аппаратные средства, осуществляющие получение, обработку и хранение измерительной информации (измерительные преобразователи, меры, средства вычислительной техники, средства и системы передачи, приема и обработки измерительной информации и другие технические средства обработки информации);

– программные средства (общесистемное и прикладное ПО, системы управления базами данных и т.п.).

При обработке измерительной информации в ИИС за счет реализации технических каналов утечки возможно возникновение таких угроз как:

– угрозы утечки акустической информации;

– угрозы утечки видовой информации;

– угрозы утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН).

Однако, несмотря на это, как раз менее вероятными угрозами в ИИС иностранного производства будут угрозы утечки информации по техническим каналам. А «слабым звеном» в этих ИИС будут являться, прежде всего, информационные технологии, программные и аппаратные средства. Соответственно, наиболее актуальными угрозами безопасности информации будут угрозы НСД к информации в ИИС.

Угрозы НСД в ИИС с применением программных и программно-аппаратных средств реализуются при осуществлении доступа и включают в себя:

– угрозы доступа (проникновения) в операционную среду ИИС с использованием штатного ПО (средств операционной системы или прикладных программ общего применения);

– угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п.;

– угрозы специального программно-технического воздействия (СПТВ) за счёт внедрения вредоносных (деструктивных) программ в программную среду ИИС или разрушающих закладных устройств непосредственно в ИИС.

Угрозы доступа (проникновения) в операционную среду ИИС и НСД к измерительной информации связаны с доступом:

– к информации и командам, хранящимся в базовой системе ввода/вывода (BIOS) ЭВМ ИИС, с возможностью перехвата управления загрузкой операционной системы и получением прав доверенного пользователя;

– в среду функционирования локальной операционной системы отдельного технического средства ИИС с возможностью выполнения НСД путем вызова штатных программ операционной системы или запуска специально разработанных программ, реализующих такие действия;

– в среду функционирования прикладных программ (например, к локальной системе управления измерительными преобразователями или мерами);

– непосредственно к измерительной информации (промежуточным и итоговым результатам) и обусловлены возможностью нарушения ее конфиденциальности, целостности и доступности.

Угрозы создания нештатных режимов работы программных (программно-аппаратных) средств – это угрозы типа «отказа в обслуживании». Как правило, данные угрозы характерны для ИИС реализованных в виде локальных и распределенных систем вне зависимости от подключения к сети информационного обмена. Их реализация обусловлена тем, что при разработке системного или прикладного ПО не учитывается возможность преднамеренных действий по целенаправленному изменению:

– содержания служебной информации в пакетах сообщений, передаваемых по измерительным каналам (сети);

– условий обработки данных измерительной информации (например, игнорирование ограничений на длину пакета сообщения);

– форматов представления данных измерительной информации (с несоответствием измененных форматов, установленных для обработки по протоколам сетевого взаимодействия);

– непосредственно ПО обработки данных в ИИС.

В результате реализации угроз типа «отказа в обслуживании» происходит переполнение буферов и блокирование процедур обработки, «зацикливание» процедур обработки и «зависание» ЭВМ ИИС и др.

Угрозы специального программно-технического воздействия – это поражение программных средств ИИС, применяемых на промышленных объектах, в учреждениях и организация, путем внедрения вредоносных (деструктивных) программ в программы ИИС или разрушающих закладных устройств непосредственно в элементы ИИС, что приводит к разрушению или искажению программ (алгоритмов) и информационных массивов, хранящихся и циркулирующих в этих системах, и исключает их нормальное функционирование. Наличие в ИИС вредоносных программ и разрушающих закладных устройств может способствовать возникновению скрытых, в том числе нетрадиционных каналов доступа к защищаемой информации, позволяющих вскрывать, обходить или блокировать защитные механизмы, предусмотренные в системе, в том числе парольную или криптографическую защиту.

В этом случае, средствами СПТВ можно считать программные, аппаратные или программно-аппаратные средства, с использованием которых может быть осуществлено несанкционированное копирование, искажение, уничтожение информации, ее передача за пределы контролируемой зоны или блокирование доступа к ней [4].

В зависимости от механизма действия средства СПТВ условно делятся на:

– специальные программы (алгоритмы) или вредоносные программы;

– разрушающие закладные устройства, в том числе и программные «закладки»;

– программные средства блокировки доступа в информационных сетях.

Проанализировав возможности средств СПТВ в [4], можно выделить такие последствия реализации данного класса угроз в ИИС как:

– нарушение целостности и конфиденциальности обрабатываемой измерительной информации;

– функциональное поражение как элементов ИИС, так ИИС в целом;

– изменение режимов работы аппаратных средств, программ, внесение ошибок в потоки обрабатываемой и передаваемой измерительной информации;

– блокировка и снижение эффективности работы сетей передачи измерительной информации;

– «засорение» свободной памяти ЭВМ ИИС, и как следствие, снижение производительности ИИС;

– уничтожение или искажение загрузочного сектора диска;

– несанкционированное форматирование жёстких дисков;

– вывод сообщений на дисплей в виде баннеров;

– блокировка клавиатуры и других устройств ввода/вывода измерительной информации;

– изменение режимов работы программ или содержимого файлов;

– выход из строя (на физическом уровне) жестких дисков и других элементов ИИС;

– психологическое воздействие на пользователей информационной системы.

Список литературы:

1. ГОСТ Р 50922- 2006. Защита информации. Основные термины и определения. – М.: Стандартинформ, 2007. – 12 с.

2. МИ 3286-2010. ГСИ. Рекомендация. Поверка защиты программного обеспечения и определения ее уровня при испытаниях средств измерений в целях утверждения типа. М.: АНО «РСК-Консалтинг», 2010. – 30 с.

3. Хорев А.А. Угрозы безопасности информации // Специальная техника. – М., 2010. – №1 – С. 50–63.

4. Смык С.В. Анализ возможностей средств специального программно-технического воздействия // Перспективы развития информационных технологий: сборник материалов XIX Международной научно-практической конференции. – Новосибирск: Изд-во ЦРНС, 2014. – №19. – С. 159–164.