УДК 004.056.53

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНОЙ СИСТЕМЫ ИВГ.1М

Ермаков В.А., Серикбаев Б.С., Ильиных С.А., Коровиков А.Г.

Институт атомной энергии НЯЦ РК, Курчатов, Казахстан

В настоящее время растет количество и значение информационных систем (ИС) на предприятиях и, как следствие, должно расти доверие пользователей к их применению. Существует ряд технологий, которые помогают обеспечить безопасность использования ИС. Однако технология сама по себе не решает всех проблем, поэтому существует необходимость в четко определенных политиках безопасности информационных систем, чтобы обеспечить конфиденциальность, целостность, доступность, безотказность и достоверность информации. В данной статье ставится задача защиты информации в измерительной системе реакторной установки ИВГ.1М от несанкционированного доступа. На примере защиты информационной системы раскрывается комплексный подход к защите информации, показано совместное проведение организационных и технических мероприятий. В статье производится анализ информационной системы, ее классификация, определение требований к ее защищенности. На основании анализа определяются специализированные средства защиты, а также организационные мероприятия, применимые к системе. В заключении раскрываются результаты применения данного подхода к защите.

Введение

С 2010 года и по настоящее время в Институте атомной энергии (ИАЭ) проводятся работы по модернизации ИИС исследовательского реактора ИВГ.1М. На сегодняшний день проведен первый и второй этап модернизации. В опытную эксплуатацию введены: система автоматического управления (САУ), система управления и защиты (СУЗ) и система контрольно-измерительных приборов и автоматики (КИПиА) [1, 2]. В качестве технических средств используются современные программные и аппаратные средства промышленной автоматики на основе микропроцессорной техники зарубежных производителей. Все системы основаны на распределенной архитектуре с использованием передачи данных через локальные вычислительные сети. Разработанные программные средства позволяют вести сбор и регистрацию параметров реактора и его систем, отображение параметров в виде графиков, таблиц, мнемосхем и гистограмм.

Актуальность работы

Сегодня ИС играют ключевую роль в обеспечении эффективной работы на производстве. Повсеместное использование ИС для хранения, обработки и передачи информации делает актуальными проблемы их защиты. Например, каждый день появляются новые вирусы, несущие новые угрозы, такие как потеря или публичное распространение информации.

Под безопасностью понимается защищенность системы от случайного или преднамеренного вмешательства в нее, попыток несанкционированного получения информации, модификации или физического разрушения ее компонентов. Под угрозой безопасности понимаются возможные события или действия, которые могут привести к искажению, несанкционированному использованию или даже к разрушению информационных ресурсов, а также программных и аппаратных средств [3].

Комплекс исследовательских реакторов (КИР) «Байкал-1» является ядерно-опасным объектом в связи с основной деятельностью в области использования атомной энергии. Основой для возникновения угроз в отношении КИР «Байкал-1» является наличие ядерных материалов и источников ионизирующего излучения, что, безусловно, связано с возрастающим интересом к ним со стороны террористических группировок и радикально настроенных экстремистов. ИИС ИВГ.1М является уязвимой в этом плане системой, основные процессы которой заключаются в сборе, регистрации и отображении параметров исследовательского реактора. Последствия угроз информационной безопасности (ИБ) в отношении ИИС могут привести к фальсификации данных, потере зарегистрированной информации и в конечном итоге, экономическим потерям от срыва контрактов и научных программ.

Анализ информационной системы

При проведении комплекса мероприятий по защите информации от несанкционированного доступа для информационной системы сначала необходимо привести аналитическое обследование, а затем реализовать для информации соответствующие требования.

Рассмотрим ИИС реакторной установки ИВГ.1М. Определим исходные данные для данной ИИС, а затем сформулируем и реализуем требования к ее защищенности.

Исходные данные к системе:

– обрабатывает информацию ограниченного пользования;

– обеспечивает многопользовательский режим работы;

– разграничивает права пользователей;

– обеспечивает коллективный режим обработки данных.

Рисунок. Средства обеспечения ИБ

На основе исходных данных должны выполняться следующие требования к ИИС:

- идентификация, проверка подлинности и контроль доступа субъектов к системе, программам, зарегистрированным данным;
- регистрация и учет входа пользователей в систему, запуска программ, изменений полномочий субъектов;
- учет носителей информации;
- регистрация попыток нарушения защиты;
- физическая защита средств вычислительной техники и носителей информации;
- наличие администратора системы;
- наличие средств восстановления программного обеспечения;
- использование сертифицированных средств защиты.

Средства обеспечения ИБ

В результате проведения анализа ИБ ИИС ИВГ.1М была определена степень защиты данной информационной системы. На рисунке приведена классификация программно-аппаратных средств ИБ, используемых в ИИС ИВГ.1М.

Программные средства защиты

Для защиты информационной системы используются специализированные программные средства защиты, позволяющие защитить рабочие станции, контроллеры и систему в целом для:

- идентификации пользователей;
- контроля доступа;
- шифрования информации;
- удаления остаточной (рабочей) информации типа временных файлов;
- тестового контроля системы защиты и др.

Преимущества программных средств: универсальность, гибкость, надежность, простота установки, способность к модификации и развитию.

Разработанное прикладное программное обеспечение (SCADA система – RSView) предусматривает авторизацию пользователей с помощью логина и пароля. Авторизация пользователя осуществляется при запуске системы. Все действия операторов после запуска программного обеспечение записываются в журнал активности.

Для защиты рабочих мест операторов от установки вредоносных программ и несанкционированного скачивания данных отключена возможность использования внешних носителей информации (USB - накопителей).

Дополнительным методом защиты информации является применение резервного копирования важной информации (конфигурации операционной системы и SCADA-системы автоматизированных рабочих мест операторов, копии конфигурации ПО контроллеров и т.д.).

Проведенные работы по защите информационно-измерительной системы

Техническим средствам защиты информации нужна непрерывная организационная поддержка, которая заключается в смене паролей, определении ролей, полномочий, разграничении доступа и т.п. Защита информации – это не разовое мероприятие, это постоянный процесс. Для обеспечения непрерывности работы средств защиты и пресечения несанкционированного доступа к системе безопасности применены следующие меры:

- определен порядок установления уровня доступа пользователей и правила разграничения доступа;
- пользователи ознакомлены с уровнем их полномочий, а также с организационно-распорядительной и рабочей документацией;
- обеспечена охрана объекта, на котором расположена защищаемая система (территория, здание, помещения, оборудование);

– организованы процедуры информационной безопасности: определены ответственные лица и администратор, осуществляющие учет, хранение и выдачу информационных носителей, паролей, ключей, приемку включаемых в ИИС новых программных средств, а также контроль за ходом технологического процесса обработки информации.

Заключение

Путем проведения организационных и технических мероприятий была достигнута цель в решении задачи информационной безопасности ИИС реакторной установки. Совокупность организационных методов и специализированных средств защиты позволяет оперативно реагировать на угрозы в процессе хранения, обработки, передачи информации, а также обеспечивать ее доступность и целостность.

Достигнута высокая степень защищенности, соответствующая требованиям стандартов безопасности МАГАТЭ.

Для решения проблемы информационной безопасности необходимо постоянное усовершенствование законодательных, организационных и программно-технических мер. Пренебрежение хотя бы одним из аспектов этой проблемы может привести к утрате или утечке информации, стоимость и роль которой в жизни современного общества приобретает все более важное значение.

Литература

1. Коровиков А.Г., Ольховик Д.А., Первый этап модернизации информационно-измерительной системы исследовательского реактора ИВГ.1М. – Вестник НЯЦ РК, 2014 г., вып. 4, с. 5-12.
2. Коровиков А.Г., Ермаков В.А., Серикбаев Б.С., Второй этап модернизации информационно-измерительной системы исследовательского реактора ИВГ.1М. – Вестник НЯЦ РК, 2016 г., вып. 3, с. 140-146.
3. Акимжанов С.А., Коровиков А.Г., Методы повышения информационной безопасности в филиале «ИАЭ» РГП НЯЦ РК. – Вестник НЯЦ РК, 2017 г., вып. 1, с. 138-142.
4. INTERNATIONAL ATOMIC ENERGY AGENCY, Instrumentation and Control Systems and Software Important to Safety for Research Reactors, IAEA Safety Standards Series No. SSG-37, IAEA, Vienna (2015).

ИВГ.1М АҚПАРАТТЫҚ-ӨЛШЕУ ЖҮЙЕСІНІҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІГІ

В.А. Ермаков, Б.С. Серикбаев, С.А. Ильиных, А.Г. Коровиков

ҚР ҰЯО «Атом энергиясы институты», Курчатов, Қазақстан

Қазіргі уақытта кәсіпорындарда ақпараттық жүйелердің (АЖ) саны және мағынасы жетіліп келеді және нәтижесі ретінде, тұтынушылардың оларды қолдануға сенімділігі де өсуі тиіс. АЖ пайдалану қауіпсіздігін қамтамасыз етуге көмектесетін бірқатар технологиялар бар. Бірақ, технология өздігінен барлық мәселелерді шешпейді, сондықтан, ақпараттың құпиялылығын, тұтастығын, қолжетімділігін, мүлтіксіздігін және анықтылығын қамтамасыз ету үшін ақпараттық жүйелер қауіпсіздігінің нақты белгіленген саясаттардың қажеттілігі болуда. Осы мақалада рұқсат етілмеген қол жеткізуден ИВГ.1М реакторлық қондырғының өлшеу жүйесінде ақпаратты қорғау міндеті қойылады. Ақпараттық жүйені қорғау үлгісінде ақпаратты қорғаудың кешендік тәсілдемесін ашады, ұйымдастырушылық және техникалық іс-шаралардың бірлесіп жүргізілуі көрсетілді. Мақалада ақпараттық жүйені талдау, оның жіктелуі, оның қорғалуына талаптарды белгілеу жүргізіледі. Талдау негізінде арнайы қорғау құралдары, және де жүйеде қолданылатын ұйымдастырушылық іс-шаралар анықталады. Қорытындысында осы тәсілдемені қорғауға қолдану нәтижелері ашылады.

INFORMATION SECURITY OF INFORMATION AND MEASURING SYSTEM OF THE IVG.1M REACTOR

V.A. Yermakov, B.S. Serikbayev, S.A. Ilinykh, A.G. Korovikov

Branch "Institute of Atomic Energy" NNC RK, Kurchatov, Kazakhstan

Currently, the quantity and importance of information systems (IS) at the enterprises is increasing and user's confidence for their application has to increase as a consequence.

However, technology does not solve all the problems itself, therefore there is a need for well-defined security strategy of IS to ensure privacy, integrity, availability, reliability and adequacy of information. This paper set the task to secure information in measuring system of IVG.1M reactor facility from unauthorized access. Example of information system security opens a complex approach to information security and presents joint organizational and engineering measures. The article performs analysis and classification of information system, determines the requirements for its security. Based on analysis, special means of protection as well as organizational measures applicable for the system are defined. Conclusion reflects results of such approach application for the security.