УДК 623.618.3

А.М. Кузьмицкий
(УО «ВА Республики Беларусь» г. Минск)

БЕЗОПАСНОСТЬ ДОСТУПА К АВТОМАТИЗИРОВАННЫМ СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ АТОМНОЙ ЭЛЕКТРОСТАНЦИИ

Реализуя требования по защите информации автоматизированной системы физической защиты (СФЗ) Белорусской АЭС следует строго учитывать требования по классификации автоматизированных систем.

Профили защиты [1, ст.6.2] разрабатываются и для трех классов объектов информатизации: А1, А2 и А3. При этом**,** минимальные требования по обеспечению безопасности информации предъявляются к классу А3, максимальные – к А1. К нему относятся объекты информатизации, на которых обрабатывается информация в пределах области действия комплекса систем безопасности объекта (КСБО), содержащая сведения, отнесенные к государственным секретам, технические средства которых размещены в пределах одной контролируемой зоны.

В общем случае для типовой компьютерной системы защиты от несанкционированных действий (НСД) должна обеспечивать идентификацию, аутентификацию пользователей при начале работы, контроль управления доступом к ресурсам и процессам, контроль целостности объектов компьютерной системы. Производится постоянное отслеживание процессов и событий компьютерной системы, а также организуется менеджмент безопасностью компьютерной системы.

В рамках системы защиты чувствительных ресурсов АС и информации от НСД реализуется комплекс программно-технических средств и организационных решений по защите СФЗ от несанкционированного действия. В комплекс интегрированы четыре подсистемы: управления доступом; регистрации и учета; криптографическая; обеспечения целостности.

Подсистема управления доступом проводит проверку подлинности и контроль доступа в систему часовых-операторов и администраторов по их идентификаторам и алфавитно-цифровым паролям условно-постоянного действия определенной символьной длины. Дополнительно проверка подлинности и контроль доступа в систему операторов и администраторов проводится по биометрическим характеристикам или специальным устройствам (жетонам, картам, электронным ключам). Администратор не должен иметь доступ к паролям операторов. В системе должны использоваться программные средства

для смены паролей самими операторами с соответствующей проверкой их уникальности и длины;

аутентификация внешних устройств системы по специальным тестам и протоколам аутентификации при каждом доступе к устройству;

контроль доступа операторов к командам управления внешними устройствами по принципу «в три руки» по паролям и таблицам санкционирования. Одним из операторов должен быть администратор [3, с.428].

Подсистема регистрации и учета осуществляет регистрацию загрузки/останова системы, рабочих станций, терминалов. В параметрах регистрации указываются время и дата загрузки/останова системы, идентификатор оператора и результат попытки загрузки/останова: успешный или неуспешный – несанкционированный, причина неуспешной попытки (неправильный идентификатор, пароль и т.п.).

В параметрах входа субъектов доступа в систему регистрации указываются время и дата входа субъекта, его идентификатор и результат попытки входа. При этом регистрация входа субъектов доступа в систему также производится с учётом снятых биометрических характеристик или специальных устройств. К командам управления внешними устройствами системы регистрация доступа осуществляется «в три руки».

Всех носители информации учитываются в журнале с регистрацией их приема и выдачи.

Криптографическая подсистема обеспечивает шифрование служебной информации СЗИ НСД (идентификаторов, паролей, таблиц санкционирования) и конфиденциальных (секретных) данных системы при их записи на накопители с использованием алгоритма ГОСТ 28147-89 [4].

Подсистема обеспечения целостности осуществляет контроль целостности СЗИ НСД при загрузке системы с помощью проверки наличия имен программ (файлов) и данных СЗИ НСД. В системе должен присутствовать администратор, ответственный за ведение СЗИ НСД, загрузку и останов системы, её восстановление и тестирование с использованием средств восстановления СЗИ НСД. Средства и порядок тестирования СЗИ НСД регламентируются заместителем начальника АЭС по режиму и физической защите.

Наряду с организационными мероприятиями осуществляется физическая охрана СВТ и носителей информации, предусматривающая контроль доступа в помещения АС СФЗ посторонних лиц, нали-

чие физических барьеров для потенциальных нарушителей.

Контроль целостности СЗИ НСД, программ и чувствительных данных системы при загрузке системы и по командам по эталонным контрольным суммам проводится с использованием имитовставки алгоритма ГОСТ 28147-89 [4]. Наиболее критичные ресурсы системы многократно резервируются, а данные архивируются.

Таким образом:

Защита системы физической является важнейшей частью общей задачи безопасности АЭС;

обеспечение безопасности информации должно осуществляется в строгом соответствии с правилами управления информационной безопасностью и требованиями режима секретности;

исполнение процедур контроля управления доступом к автоматизированным системам СФЗ, является наиболее важным компонентом политики информационной безопасности.

ЛИТЕРАТУРА

1. СТБ 34.101.30-2007. Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация. Национальный Интернет-портал Республики Беларусь [Электронный ресурс] / Нац. фонд технических нормативных актов Респ. Беларусь. – Минск, 2015. – Режим доступа: http://www.tnpa.by/KartochkaDoc.php?UrlRN=198020&UrlIDGLOBAL=295376. – Дата доступа: 25.05.2015.

2. Голиков, В.Ф. Безопасность информации и надежность компьютерных систем: пособ. для студентов специальностей 1-40-1 01 01 и 1-53 01 02 в 2 ч / В.Ф.Голиков. – Минск, БНТУ, 2010. ч.1. – 86с.

3. Погожин, Н.С. Физическая защита ядерных объектов. Учебник для высших учебных заведений / П.В.Бондарев, А.В.Измайлов, А.И.Толстой; под ред. Н.С.Погожина. – М.: МИФИ, 2004. – 459 с.

4. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Национальный Интернет-портал Республики Беларусь [Электронный ресурс] / Нац. фонд технических нормативных актов Респ. Беларусь. – Минск, 2015. Режим доступа: http://www.tnpa.by/KartochkaDoc.php?UrlRN=12812&UrlIDGLOBAL=12812. – Дата доступа: 25.05.2015. ~