ОРГАНИЗАЦИЯ ДОСТУПА К АВТОМАТИЗИРОВАННЫМ СИСТЕМАМ ФИЗИЧЕСКОЙ ЗАЩИТЫ АТОМНОЙ ЭЛЕКТРОСТАНЦИИ

А. М. Кузьмицкий
Кафедра специальных и инженерно-технических дисциплин учреждения образования «Военная академия Республики Беларусь»
Минск, Республика Беларусь
E-mail: a_kuzm@tut.by

В статье излагаются требования к проведению организационных мероприятий по предотвращению утечки информации или исключению воздействия на нее по техническим каналам в процессе функционирования системы физической защиты объектов использования атомной энергии.

При разработке, создании и эксплуатации автоматизированной системы физической защиты (СФЗ) Белорусской АЭС, реализующей требования по защите информации, а также для органов контроля за состоянием СФЗ и ее подсистемы защиты информации (ЗИ) необходимо учитывать требования по классификации автоматизированных систем (АС). Требования сформулированы в [1, ст.6.4], а также в [2, ст.14], которые устанавливают классификацию автоматизированных систем управления и обеспечения физической защиты ядерно-опасных объектов на базе средств вычислительной техники. Устанавливаются следующие классы объектов информатизации, для которых разрабатываются профили защиты [1, ст.6.2]:

класс А1 – совокупность объектов информатизации, на которых обрабатывается информация в пределах области действия комплекса средств безопасности объекта (КСБО), содержащая сведения, отнесенные к государственным секретам, технические средства которых размещены в пределах одной контролируемой зоны;

класс А2 – совокупность объектов информатизации, на которых обрабатывается информация в пределах области действия КСБО, содержащая сведения, отнесенные к служебной информации ограниченного распространения, технические средства которых размещены в пределах одной контролируемой зоны;

класс А3 – совокупность объектов информатизации, на которых обрабатывается открытая информация в пределах области действия КСБО, технические средства которых размещены в пределах одной контролируемой зоны.

Таким образом, минимальные требования по обеспечению безопасности информации предъявляются к классу А3, максимальные – к А1. в общем случае для типовой компьютерной системы защиты от НСД должна обеспечивать:

1. Идентификацию и аутентификацию пользователя.

2. Управление доступом к ресурсам и процессам компьютерной системы.

3. Контроль целостности объектов компьютерной системы.

4. Мониторинг процессов и событий компьютерной системы.

5. Управление безопасностью компьютерной системы.

Комплекс программно-технических средств и организационных решений по защите чувствительных ресурсов АС СФЗ от несанкционированного действия (НСД) реализуется в рамках системы защиты информации от НСД, состоящей из четырех подсистем: управления доступом; регистрации и учета; криптографической; обеспечения целостности.

Подсистема управления доступом. Должна проводиться проверка подлинности и контроль доступа в систему часовых-операторов и администраторов по их идентификаторам и паролям условно-постоянного действия длиной не менее 6 алфавитно-цифровых символов. Проводится контроль доступа администратора к программной загрузке и останову системы по паролю и списку доступа. Доступ к загрузке и останову должен иметь только администратор. Проводится аутентификация терминалов и внешних устройств системы по их логическим или физическим адресам во время загрузки. Дополнительно СЗИ НСД должна обеспечивать:

проверку подлинности и контроль доступа в систему и доступа к загрузке/останову системы операторов и администраторов по биометрическим характеристикам или специальным устройствам (жетонам, картам, электронным ключам) и паролям. Администратор не должен иметь доступ к паролям операторов. В системе используются 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 санкци-

онирования. Одним из операторов должен быть администратор [3, с.428].

Подсистема регистрации и учета. Должна осуществляться регистрация загрузки/останова системы, рабочих станций, терминалов. В параметрах регистрации указываются:

время и дата загрузки/останова системы, рабочих станций, терминалов;

идентификатор оператора (администратора);

результат попытки загрузки/останова: успешный или неуспешный – несанкционированный, причина неуспешной попытки (неправильный идентификатор, пароль и т.п.).

Должна осуществляться регистрация входа субъектов доступа в систему. В параметрах регистрации указываются:

время и дата входа субъекта доступа в систему;

идентификатор субъекта доступа;

результат попытки входа: успешный или неуспешный – несанкционированный, причина неуспешной попытки.

Должен проводиться учет всех носителей информации с регистрацией в журнале их выдачи/приема. Дополнительно СЗИ НСД должна обеспечивать:

1. Регистрацию входа субъектов доступа в систему с учётом снятых биометрических характеристик или специальных устройств и паролей. В параметрах регистрации указываются: время и дата входа/выхода субъекта доступа в систему/из системы; идентификатор субъекта доступа; результат попытки входа.

2. Регистрацию доступа «в три руки» к командам управления внешними устройствами системы. В параметрах регистрации указываются: время и дата попытки выдачи команды устройства; идентификатор (адрес, имя) устройства; идентификаторы (имена) операторов-участников (3-х); вид запрошенной команды; результат попытки: успешный или неуспешный - несанкционированный.

3. Регистрацию изменения конфигурации системы. В параметрах регистрации указываются: время и дата внесения изменения; идентификатор администратора; вид изменения конфигурации (добавление, исключение внешних устройств, изменение режимов функционирования и т.п.).

Криптографическая подсистема. СЗИ НСД должна обеспечивать 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. Должен проводится контроль целостности СЗИ НСД при загрузке системы с помощью проверки наличия имен программ (файлов) и данных СЗИ НСД. В системе необходимо присутствовие администратора, ответственного за ведение СЗИ НСД, загрузку и останов системы, её восстановление и тестирование. В системе должны иметься средства восстановления СЗИ НСД. В системе должны быть регламентированы средства и порядок тестирования СЗИ НСД. Осуществляется физическая охрана СВТ и носителей информации, предусматривающая контроль доступа в помещения АС СФЗ посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации. Должны использоваться сертифицированные СЗИ НСД. Дополнительно СЗИ НСД должна обеспечивать контроль целостности СЗИ НСД, программ и чувствительных данных системы при загрузке системы и по командам по эталонным контрольным суммам с использованием имитовставки алгоритма ГОСТ 28147-89 [4]. Наиболее критичные ресурсы системы (устройства, каналы связи и данные) многократно резервируются в «горячем режиме», а все данные и программы системы архивируются в автоматическом режиме .

Выводы:

Защита СФЗ от НСД является важнейшей частью общей задачи обеспечения безопасности информации и осуществляется согласно правилам управления информационной безопасностью и требованиям режима секретности, действующим на АЭС.

Выполнение требований по организации доступа к автоматизированным системам СФЗ, является наиболее значимым компонентом политики информационной безопасности.

1. СТБ 34.101.30-2007. Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация. Нац. Интернет-портал Респ. Беларусь [Электронный ресурс] / Нац. фонд технических нормативных актов Респ. Беларусь. – Минск, 2015. – Режим доступа: http://www.tnpa.by/KartochkaDoc.php. – Дата доступа: 25.05.2015.
2. Рук. документ Гостехкомиссии Российской Федерации «Защита от несанкционированного доступа к информации. Термины и определения». Режим доступа: http://www.iso27000.ru/zakonodatelstvo/normativnye-dokumenty-fstek-rossii/rukovodyaschii-dokument. – Дата доступа: 25.05.2015
3. 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.
4. 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.
5. 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. – Дата доступа: 25.05.2015.