$$\overline{A} = \overline{A}_1 + \overline{A}_2, \quad (3)$$

где $\overline{A}_1$ - сообщение не содержит атаку, $\overline{A}_2$ - сообщение содержит атаку, но она не обнаружена активными элементами межсетевого экрана.

$$P(\overline{A}_1) = 1 - P_a \quad (4)$$

Найдём $P(\overline{A}_2)$. Для этого надо умножить вероятность того, что сообщение содержит атаку на вероятность того, что эта атака не будет обнаружена активными элементами. Вероятность того, что атака не будет обнаружена равна $(1-P_{pf})*$ $*(1-P_{ag})*(1-P_{ids})$. Отсюда

$$P(\overline{A}_2) = P_a[(1-\mathrm{P_{pf}})*(1-\mathrm{P_{ag}})*(1-\mathrm{P_{ids}})];$$

$$P(\overline{A}) = P(\overline{A}_1) + P(\overline{A}_2) = 1 - P_a + P_a[(1-P_{pf})]*(1-P_{ag})*(1-P_{ids}) =$$

0,93224.

Вероятность того, что атака будет обнаружена активными элементами межсетевого экрана $P(A) = 1 - P(\overline{A})$ = 0,06776.

Для сравнения, вероятность обнаружения атаки из заданного множества атак ***A*** только при использовании пакетного фильтра составляет 0,022.

Предложенная архитектура межсетевого экрана позволяет создать межсетевой экран, который сочетает в себе функции пакетного фильтра и шлюза прикладного уровня.

Кроме того, отличительной особенностью такого межсетевого экрана является использование интегрированных систем обнаружения вторжений и почтового фильтра, что позволяет обеспечить максимальную безопасность корпоративных сетей при их взаимодействии с публичными и общедоступными сетями.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Олифер В.Г., Олифер Н.А.* Компьютерные сети - СПб: Питер, 2001. - 864 с.

2. *Лукацкий А.В.* Firewall – не панацея. - http://www.citforum.ru

3. *Польман Н., Кразерс Т.* Архитектура брандмауэров для сетей предприятия / Пер. с англ. - М.: Изд. дом «Вильямс». 2003. - 432 с.

4. *Лукацкий А.В.* Новые грани обнаружения и отражения угроз. - http://www.citforum.ru

М.К. Климов
Россия, г. Ростов-на-Дону, РВИ РВ

ЗАЩИТА ИНФОРМАЦИИ В КРИТИЧЕСКИ ВАЖНЫХ СЕГМЕНТАХ СИСТЕМ АВТОНОМНОГО ЭЛЕКТРОСНАБЖЕНИЯ С КОМПЬЮТЕРИЗИРОВАННЫМ УПРАВЛЕНИЕМ

В настоящее время критически важные сегменты (средства управления) систем автономного электроснабжения с компьютеризированным управлением предназначены для выполнения весьма ответственных задач обеспечения гарантированного электроснабжения объектов и комплексов специального назначения. Сис-

темы автономного электроснабжения состоят из энергетических силовых установок и средств управления ими. Они полностью автоматизированы.

Чтобы обеспечить высокую надежность и более гибкое управление системой автономного электроснабжения осуществляют компьютеризацию средств управления путем внедрения цифровой аппаратуры со специальным программным обеспечением (СПО).

Для того чтобы компьютеризированная система автономного электроснабжения (КСАЭ) функционировала в автоматическом режиме и была управляема, необходимо:

- контролировать с помощью датчиков параметры КСАЭ, например, напряжение, частоту тока, мощность, время работы;
- осуществлять сбор и обработку информации, получаемой от датчиков КСАЭ, доставлять эти данные по каналам связи в автоматизированное рабочее место (АРМ) пункта управления;
- производить сравнение текущих значений параметров КСАЭ с базой данных эталонных значений;
- вычислять разностный сигнал для автоматизированного оптимального управления КСАЭ.

Схема защиты информации критически важных сегментов перспективных систем автономного электроснабжения с компьютеризированным управлением представлена на рис.1.

Специфической особенностью критически важных сегментов КСАЭ является то, что информация управления, расчетные программы и микропроцессорные устройства непосредственно управляют электроустановкой в реальном масштабе времени. Наиболее опасной угрозой является несанкционированное включение электроустановки путем использования уязвимостей в тракте сбора, передачи и выдачи информации на пункт управления. Нарушение функционирования КСАЭ можно считать наиболее существенным фактором преднамеренного вывода из строя объектов и комплексов специального назначения.

Объектом защиты в КСАЭ является технологическая информация, включающая:

- оцифрованные сигналы от датчиков, контролирующих необходимые параметры КСАЭ;
- базу эталонных параметров КСАЭ;
- пакеты данных, получаемые с пункта управления КСАЭ и передаваемые на него по проводным и радиоканалам связи, обеспечивающих программное управление функционированием КСАЭ;
- данные, используемые для цифрового программного управления адаптером, обеспечивающим информационное взаимодействие между датчиками и интерфейсами АРМ со средствами формирования сигналов управления КСАЭ;
- сведения о нештатных ситуациях в КСАЭ, например, несанкционированное ее включение или выключение.

Нарушение безопасности информации в КСАЭ может произойти путем:

- внедрения ложных программ и эталонных параметров,
- программно-технического воздействия (ПТВ) на сигналы управления КСАЭ, передаваемые по различным технологическим каналам.

Все эти воздействия могут привести к частичному либо полному нарушению технологического процесса управления КСАЭ.

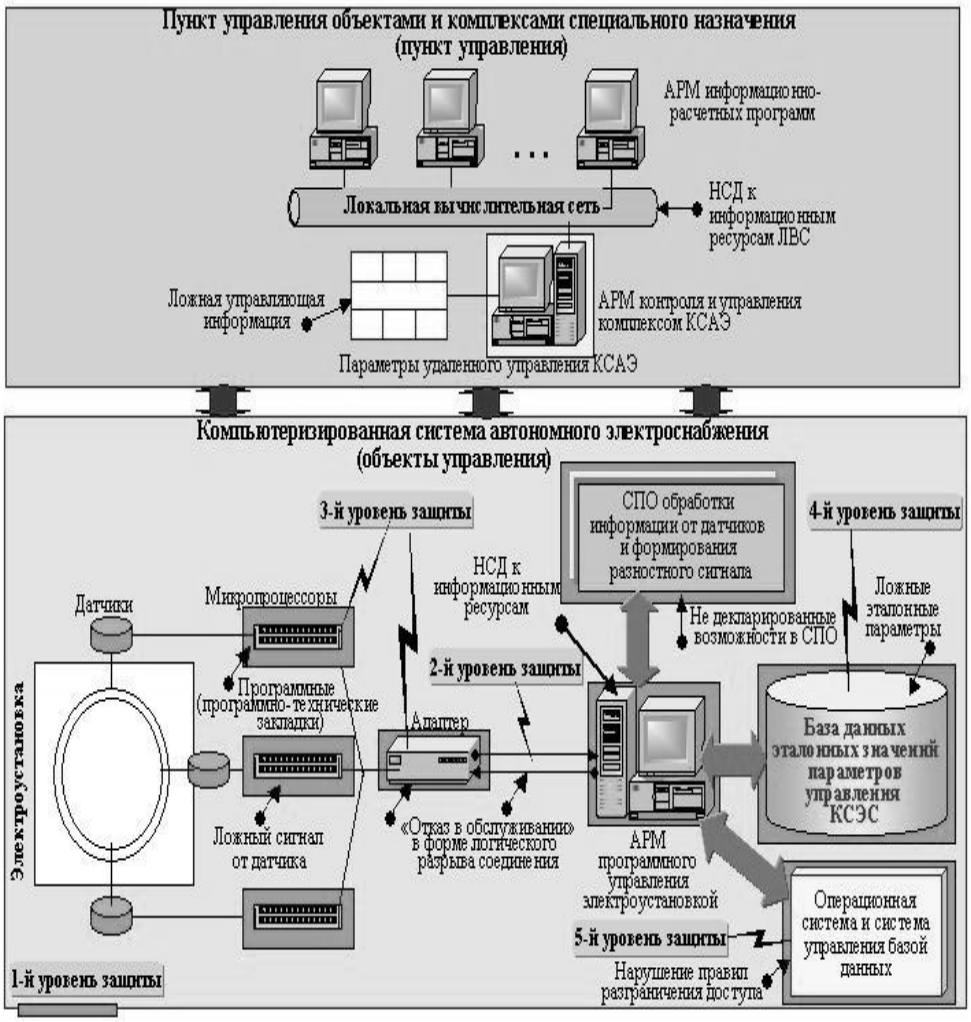

Рис. 1. Схема защиты информации критически важных сегментов перспективных систем автономного электроснабжения с компьютерным управлением

На схеме приняты обозначения:

- уязвимые места КСАЭ;
- критически важные сегменты КСАЭ.

Опасность нарушения функционирования КСАЭ состоит в том, что измеряемые ее параметры не носят строго конфиденциальный характер. Преднамеренное искажение этих значений или деструктивное программно-техническое воздействие на базу эталонных данных и на передаваемую в каналах связи информацию о сигналах управления дезорганизует работу КСАЭ и, как следствие, приводит к полному выводу ее из строя.

При разработке средств защиты информации для инфраструктуры КСАЭ ее уровни защиты от угроз безопасности информации могут реализовываться следующим образом (рис.1):

- контролем физического доступа к элементам КСАЭ путем организации технических мероприятий по недопущению посторонних лиц (1- й уровень);

- защитой доступа к информации, передаваемой по различным технологическим проводным и радиоканалам связи, установкой в коммуникационном оборудовании программных (программно-технических) средств разграничения доступа к сигналам управления КСАЭ (2 - й уровень);

- защитой информации в микропроцессорных устройствах и адаптерах с цифровым программным управлением путем специальных проверок микропроцессорных устройств и адаптеров на предмет наличия не декларированных возможностей (3 - й уровень);

- защитой базы данных эталонных контролируемых параметров и специального программного обеспечения обработки информации о сигналах управления КСАЭ, формируемых в АРМ пункта управления, от несанкционированного доступа (НСД) и ПТВ путем внедрения сертифицированных программных (программно-технических) средств защиты информации (4 - й уровень);

- защитой информации от НСД, ПТВ и воздействия компьютерных вирусов на уровне общего программного обеспечения АРМ пункта управления путем настройки средств защиты информации операционной системы, системы управления базой данных и установки антивирусных программ (5 - й уровень).

Контролируемыми параметрами (событиями безопасности) при реализации уровней защиты информации в КСАЭ и проверке порядка функционирования являются: время запуска или переключения системы, допустимые значения параметров (напряжение, частоту тока, мощность и т.д.) при переводе системы в различные режимы функционирования и номинальные значения параметров при штатной работе КСАЭ.

Таким образом, к наиболее опасным угрозам нарушения безопасности информации в КСАЭ следует отнести несанкционированное включение, искажение сигналов от датчиков и нарушение проверочных данных. Реализацию защищенного информационного тракта в КСАЭ целесообразно осуществлять на основе комплексного использования средств защиты информации на всех уровнях протоколов передачи данных и разработки специального программного обеспечения в защищенном исполнении и средств защиты информации АРМ пункта управления и КСАЭ.