УДК 005:681.516.7

А.Н. Давиденко, Ю.В. Мякухин,
НАН Украины ИПМЭ им. Г.Э. Пухова, г. Киев.

ПРОВЕДЕНИЕ КЛАССИФИКАЦИИ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПА ПРИ ЗАЩИТЕ СЛОЖНЫХ ЭНЕРГЕТИЧЕСКИХ ОБЪЕКТОВ

In article is founded proved of application classification and given classification of control devices management of access to different characteristics.

Объекты энергетики сложные по структуре и инфраструктуре инженерно-технические сооружения с большим числом обслуживающего персонала. Такие объекты как АЭС, ГЕС, ТЕС являются потенциально опасными объектами, поскольку при выходе из строя кого-либо технологического оборудования может привести к возникновению чрезвычайной ситуации (ЧС) в масштабах мира. При недостаточном контроле доступа к некоторым технологическим системам это может привести к ЧС. Вывод из строя некоторого технологического оборудования может осуществляться как преднамеренно, так и случайно. Осуществлять это могут как обслуживающий персонал объекта так посторонние лица.

В разных государствах, и частности в Украине, в настоящее время на сложных энергетических объектах могут возникнуть в любое время техногенные чрезвычайные ситуации. Это обусловлено рядом причин, которые приведены ниже. Это следующие причины:

— тенденция возрастания краж наиболее ценных материально-технических ресурсов с предприятий;
— тенденция возрастания социальной напряженности в государстве;
— возможные акты терроризма на технологических объектах;
— тенденция возрастания криминогенной обстановки в государстве;
— приход на свободные рабочие места неквалифицированных сотрудников.

Для предотвращения чрезвычайных ситуаций и повышения безопасного функционирования энергетических объектов могут проводится ряд мероприятий, это следующие:

— физические;
— организационные;
— законодательные;
— административные;
— морально-этические;
— технические;
— комбинированные.

В рамках данной работы рассмотрим технические мероприятия для

осуществления безопасности энергетического объекта. К этим мероприятиям можно отнести оснащение конкретного объекта техническими средствами охраны. Одним из видов оснащения этих средств охраны является внедрение систем контроля и управления доступом (СКУД).

Для того, чтобы принять правильное техническое решение о внедрении СКУД на сложные энергетические объекты, необходимо четко знать такие главные факторы: против кого и чего защищать, что и как защищать, хорошо быть осведомленным в знании законодательных и нормативных документов в энергетической отрасли, характер и месторасположение объекта энергетики, от каких угроз защищать, знать, на сколько хорошо защищен объект до и после внедрения СКУД.

В мире существует большое количество средств и систем контроля и управления доступом (КУД) все они отличаются по своей природе. Для того чтобы с большей степенью защитить распределенный в пространстве энергетический объект СКУД, большую роль играет классификация средств КУД и СКУД. При защите объектов энергетики от несанкционированного проникновения на территорию или в отдельные помещения обслуживающего персонала или посторонних лиц, надо знать, в каких случаях необходимо применять те или иные средства КУД или же применять СКУД. И для того, чтобы правильно принять техническое решение о выборе конкретного СКУД, надо определить по каким отличительным признакам можно его осуществить.

Контроль и управление доступом (КУД) - комплекс мероприятий, направленных на ограничение и санкционирование доступа людей, транспорта и других объектов в/из помещения, здания, зоны и территории [3].

При этом следует различать понятия средства КУД от СКУД. Главным отличием этих инженерно-технических устройств заключается в том, что средства КУД – те технические средства (радиоэлектронные, механические, электромеханические и инженерные), которые могут входить в состав КУД, а СКУД – это система, являющаяся совокупностью средств контроля и управления, обладающих технической, информационной, программной и эксплуатационной совместимостью.

Для решения задачи выбора и обоснования целесообразности применения конкретного средства КУД при проектировании и модернизации СКУД энергетических объектов, авторами была разработана классификация средств КУД и СКУД на основе открытых источников информации [1 - 6].

Рассмотрим классификационные признаки средств и систем КУД.

Вначале остановимся на средствах КУД. По проведению организационно-технических мероприятий комплекса КУД делятся на: организационные, технические, организационно-технические.

По количеству контролируемых точек доступа средств КУД и СКУД: многопропускные, однопропускные.

По количеству управляемых средств КУД на одном пропускном пункте:

одноисполнительные, многоисполнительные.

По степени инженерно-технических решений средств КУД делятся на: инженерные, электромеханические, радиоэлектронные.

Инженерные средства СКД делятся на: ворота, двери, шлагбаумы, турникеты, калитки.

Ворота и двери по виду открытия подразделяются на: распашные односторонние, распашные двухсторонние, раздвижные односторонние, раздвижные двухсторонние.

Турникеты классифицируются по таким видам: тумбовые, триподы, полуростовые роторные, полноростовые роторные.

Калитки (ворота, двери, шлагбаумы) классифицируются по степени механизации на: электромеханические, механические.

По виду перекрытия проема или прохода калитки (турнекеты) делятся на: полуростовые, полноростовые.

По физическому принципу действия средства КУД делятся на: электромагнитные, электромеханические, биометрические, оптические, механические, акустические, электронные, комбинированные.

Электромагнитные СКД классифицируются на: контактные, безконтактные.

Безконтактные СКД могут быть таких видов: в виде магнитных карточек, в виде магнитных брелков, в виде магнитных браслетов.

По разграничению доступа к определенной территории объекта различают средства КУД и СКУД: с разграничением, без разграничения.

Средства КУД классифицируют по: функциональному назначению устройств, устойчивости к несанкционированному действию.

Средства КУД по функциональному назначению устройств подразделяют на: устройства преграждающие управляемые (УПУ) в составе преграждающих конструкций и исполнительных устройств, устройства ввода идентификационных признаков (УВИП) в составе считывателей и идентификаторов, устройства управления (УУ) в составе аппаратных и программных средств, комбинированных средств.

УПУ классифицируют по: виду перекрытия проема прохода, по способу управления.

По виду перекрытия проема прохода УПУ могут быть: с частичным перекрытием (турникеты, шлагбаумы), с полным перекрытием (сплошные двери, ворота), с блокированием объекта в проеме (шлюзы, кабины проходные).

По способу управления УПУ могут быть: с ручным управлением, с полуавтоматическим управлением, с автоматическим управлением, комбинированным управлением.

По виду преграждающих конструкций (назначению) УПУ: для ограничения доступа перемещения людей и передвижения транспорта;

По виду исполнительного механизма: с использованием управляемых

приводов и управляемых блокирующих устройств.

По наличию в УПУ дополнительных устройств:

— средств охранной сигнализации;
— средств светового и/или звукового оповещения;
— средств досмотра;
— антипаниковых устройств;
— датчиков контроля и счетчиков прохода одного или более лиц, перемещения транспортных средств;
— датчиков сигнализации перемещения и конечного положения подвижных преграждающих конструкций.

По выполнению основных функций средств КУД: энергоснабжению, защите от неправомерного вторжения, защите от несанкционированного доступа, управлению пунктами доступа, идентификации (опознавании), индикации, сигнализации, обмен информацией с другими системами безопасности.

УВИП классифицируют по следующим признакам: по виду используемых идентификационных признаков, по способу считывания идентификационных признаков, комбинированные.

По виду используемых идентификационных признаков УВИП могут быть:

— механические - идентификационные признаки представляют собой элементы конструкции идентификаторов (перфорационные отверстия, элементы механических ключей и т.д.);
— магнитные - идентификационные признаки представляют собой намагниченные участки поверхности или магнитные элементы идентификатора (карты с магнитной полосой, карты Виганда и т. д.);
— оптические - идентификационные признаки представляют собой нанесенные на поверхности или внутри идентификатора метки, имеющие различные оптические характеристики в отраженном или проходящем оптическом излучении (карты со штриховым кодом, голографические метки и т. д.);
— электронные - идентификационные признаки представляют собой электронный код, записанный в электронной микросхеме идентификатора (дистанционные карты, электронные ключи и т. д.);
— акустические - идентификационные признаки представляют собой кодированный акустический сигнал;
— биометрические - идентификационные признаки представляют собой индивидуальные физические признаки человека (отпечатки пальцев, геометрия ладони, рисунок сетчатки глаза, голос, динамика подписи и т.д.);
— комбинированные - для идентификации используются одновременно несколько идентификационных признаков.

По способу считывания идентификационных признаков УВИП могут

быть:

— с ручным вводом - ввод производится с помощью нажатия клавиш, поворотом переключателей или других подобных элементов;
— контактные - ввод происходит при непосредственном, в том числе и при электрическом, контакте между считывателем и идентификатором;
— дистанционные (бесконтактные) - считывание кода происходит при поднесении идентификатора на определенное расстояние к считывателю;
— комбинированные.

Безконтактные считыватели по дальности действия подразделяются на: малой дальности, средней дальности, большой дальности.

По типу идентификаторов, питающиеся от напряжения подразделяются на: пассивные, активные.

По свойству реализации и управления УУ: аппаратные, программные, программно-аппаратные средства.

По предотвращению или затруднению несанкционированного доступа к каким – либо ресурсам: программные, технические, программно-технические.

Сюда также относятся специальные защитные знаки (СЗЗ) [6]. СЗЗ представляют собой продукты, созданные на основе физико-химических технологий и предназначенные для контроля доступа к объектам защиты, а также для защиты документов, идентифицирующих личность, от подделки.

По способу разрешения санкционированного доступа посторонних лиц, одноразово посещающих конкретные лица обслуживающего персонала технологического объекта подразделяются на:

— с рабочих мест без согласования со службой безопасности объекта и начальником подразделения;
— с рабочих мест с согласованием со службой безопасности объекта и начальником подразделения
— в службе безопасности объекта с согласованием начальника подразделения.

Далее рассмотрим классификационные признаки СКУД. СКУД можно классифицировать по таким основным признакам:

— способу управления;
— количеству контролируемых точек доступа;
— функциональным характеристикам;
— виду объектов контроля;
— уровню защищенности системы от несанкционированного доступа к информации.

По способу управления СКУД:

— автономные - для управления одним или несколькими УПУ без передачи информации на центральный пульт и без контроля со стороны оператора;
— централизованные (сетевые) -для управления УПУ с обменом информацией с центральным пультом и контролем и управлением

системой со стороны оператора;

— универсальные - включающие функции как автономных, так и сетевых систем, работающие в сетевом режиме под управлением центрального устройства управления и переходящие в автономный режим при возникновении отказов в сетевом оборудовании, в центральном устройстве или обрыве связи.
— контроль и управление доступом удаленных объектов, а также являющиеся частью интегрированной системой охраны или комплексной системы охраны системой охраны.

По количеству контролируемых точек доступа: малой емкости (менее 16 точек), средней емкости (не менее 16 и не более 64 точек), большой емкости (64 точки и более).

По функциональным характеристикам СКУД:

— по основным функциональным характеристикам для каждого класса СКУД (для автономных систем, систем с централизованным управлением и универсальных);
— по сервисным или дополнительным показателям;
— системы ограничения доступа (предполагая системы домофонного вида);
— системы контроля доступа с устройствами досмотра. Последние, в частности, могут быть применены для контроля за перемещением предметов из одной зоны в другую с целью проверки наличия/ отсутствия опасных или несанкционированных веществ, материалов, которые делятся на:
— системы с ограниченными функциями;
— системы с расширенными функциями;
— многофункциональные системы.

По наличию основных функциональных характеристик СКУД (автономных систем, систем с централизованным управлением и универсальных), представленных по трем классам на обязательные или преимущественные и сервисные или дополнительные показатели.

Для системы, которая планируется внедряться на объекты или помещения с повышенными требованиями по условиям доступа по таким показателям.

— доступ по правилу «двух и более лиц»;
— ввод специального идентификационного признака для открывания под принуждением;
— применение биометрических идентификаторов;
— защиту от повторного использования идентификатора для прохода в одном направлении;
— контроль за перемещением посетителей по контролируемым зонам.
— уровнем защищенности идентификации объектов, реализуемые соотношением между числом различных возможностей кодирования и числом идентифицируемых пользователей;

— по контролю доступом к информации или в помещение.

По виду объектов контроля СКУД: для контроля доступа физических объектов, для контроля доступа к информации.

Классификация СКУД по устойчивости к НСД. СКУД классифицируют по такой степени устойчивости к НСД: нормальной, повышенной, высокой.

По типу устойчивости к воздействию: разрушающему, неразрушающему.

УПУ и УВИП классифицируют по устойчивости к разрушающим воздействиям. Устойчивость УПУ устанавливают по: устойчивости к взлому, пулестойкости, устойчивости к взрыву.

Устойчивость УВИП устанавливают по устойчивости считывателя к взлому. Для УПУ повышенной и высокой устойчивости устанавливают дополнительно 5 классов по показателям устойчивости (1-й класс - низший).

По устойчивости к неразрушающим воздействиям средств и систем КУД в зависимости от их функционального назначения:

— устойчивости к вскрытию - для УПУ и исполнительных устройств (замков и запорных механизмов);
— устойчивости к манипулированию;
— устойчивости к наблюдению - для УВИП с запоминаемым кодом (клавиатуры, кодовые переключатели и т.п.);
— устойчивости к копированию (для идентификаторов);
— устойчивости защиты средств вычислительной техники УУ от несанкционированного доступа к информации.

Проведенная классификация технических средств позволяет выбрать для конкретного технологического объекта необходимые технические средства КУД, с учетом предполагаемых уязвимых мест в работе этих устройств в случае реализации ожидаемых угроз.

1. Электронный ресурс. Определение, классификация систем контроля доступа (СКД). Режим доступа http://l2b.ru/articles/01072/152/ru-ru/
2. Электронный ресурс. Биометрические системы контроля доступа и учёта рабочего времени персонала. Режим доступа http://www.podkontrolem.ru/control-bio.html.
3. ГОСТ Р 51241-98. Средства и системы контроля и управления доступом: классификация. Общие технические требования. Методы испытаний.
4. Электронный ресурс. Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации. Гостехкомиссия России. М.: 1992. Режим доступа http://linux.nist.fss.ru/hr/doc/gtk/gtk014.htm
5. Электронный ресурс. Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требований по защите информации. Гостехкомиссия России. М.: 1992. Режим доступа http://linux.nist.fss.ru/hr/doc/gtk/gtk009.htm
6. Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования. Гостехкомиссия России. М.: 1997.

Поступила 22.01.2009р.