Выпуск 25 · часть 1

Узкополосная ТЕХНОЛОГИЧЕСКАЯ РАДИОСЕТЬ УКВ диапазона для полигонных комплексов различного назначения

ООО «НЦПР» (Технический бюллетень)

В настоящей статье представлена краткая информация о технологических радиосетях управления и сбора данных на узкополосных радиомодемах диапазона ультракоротких волн (УКВ), обеспечивающих функционирование военных и гражданских полигонов различного назначения. Статья предназначена для руководителей и технических специалистов, связанных с созданием и эксплуатацией распределенных автоматизированных систем удаленного управления и сбора данных наземного (надводного) и воздушного базирования.

1. Общая информация

Слово «полигон» имеет различные значения. В настоящей статье рассматриваются объекты, которые наиболее точно определены в Большой советской энциклопедии[1]. Но кроме упомянутых ниже военных полигонов, рассматривается также оснащение и гражданских полигонов, включая полигоны твердых бытовых отходов (ТБО).

Испытательная площадка ЗРК полигона «Капустин Яр»

(www.topwar.ru/68532-sovetskie-i-rossiyskie-poligony-i-ispytatelnye-centry-na-snimkah-google-earth.html)

Технологические радиосети[2] обмена данными для всех типов полигонов имеют много общего, но рассматриваются в различных разделах настоящей статьи, чтобы корректнее представить информацию для различных целевых аудиторий.

Общими характеристиками и требованиями практически всех полигонов являются:

- значительная площадь. Например, общая площадь широко известного полигона «Капустин Яр»[3] составляет 650 км² (ранее занимал площадь около 0,40 млн га);
- размещение на значительном удалении от крупных населенных пунктов;
- наличие на территории полигона подлежащих контролю как стационарных, так и подвижных объектов;
- обеспечение безопасности работы как на самом полигоне, так и по его периметру.

Вышеуказанные характеристики, наряду с назначением и функциональными возможностями определяют требования к системе связи на таких объектах.

2. Система связи полигона

Система связи полигона, как правило, строится на проводных и беспроводных средствах. Целесообразность и необходимость применения беспроводных средств определяется, в первую очередь, размерами оперативной зоны, на которой они должны функционировать, что и понятно, поскольку организация применения проводных средств связи для работы на десятки километров оказывается более сложной и менее привлекательной с экономической точки зрения. Достаточно сравнить сроки развертывания и затраты на создание и, главное, содержание кабельной системы, укладываемой в потерны или траншеи, чтобы, что называется, «почувствовать разницу».

Решение значительной части функциональных задач на полигоне может обеспечиваться сетями общего пользования (например, средствами сотовой связи). Однако, размещение полигонов вдали от крупных населенных пунктов делает их мало привлекательными для включения в зону действия таких сетей. Кроме того, использование технологической радиосети в этом случае представляется более безопасным и надёжным. А в отдельных случаях и безальтернативным, поскольку такая радиосеть позволяет работать в режиме реального времени и со строго детерминированными задержками в доставке информации, что критично для функционирования различных полигонных автоматизированных систем. Например, использование радиосети для передачи сигналов единого времени для синхронизации работы полигонных комплексов давно стало стандартом де-факто.

Задачи управления и контроля работы подвижных объектов (наземных, надводных, воздушных и, частично, подводных/полупогружаемых) на полигоне могут решаться только с использованием средств технологической радиосети. Наиболее широкое распространение на полигонах получили узкополосные радиосети УКВ диапазона[4], обеспечивающие надежную работу на приемлемую для таких объектов дальность — номинальный радиус зоны действия с позиции только одной базовой станции составляет около 25 км, что соответствует площади около 2000 км^2, для наземных (надводных) и около 350 км (400 тыс. км^2) для высотных воздушных объектов.

Высокая безопасность технологических радиосетей обмена данными УКВ диапазона обеспечивается применением аппаратуры, предназначенной для работы в диапазонах радиочастот (обычно ОВЧ и УВЧ), не предназначенных для использования другими пользователями и контролируемых соответствующими регулирующими органами. Несомненно, радиосредства имеют более низкие параметры в части скрытности работы по сравнению с проводными (кабельными) средствами связи, но получение доступа к циркулирующей в такой радиосети информации или срыв ее работы оказываются не такой уж простой задачей.

Следует отметить, что защита данных в любой системе представляет собой непрерывный комплекс организационно-технических и специальных мероприятий, ни одно из которых самостоятельно не позволяет добиться поставленной задачи. Тем не менее, средства узкополосной технологической радиосети обмена данными УКВ диапазона изначально обладают свойствами, позволяющими существенно снизить существующие угрозы.

Безопасность данных в стационарных и подвижных технологических радиосетях для полигонов является одним из ключевых условий их использования, а строительство таких радиосетей осуществляется с учетом полного исключения или максимального затруднения компрометации циркулирующей в них информации. В радиосетях обмена данными широко применяются различные методы и способы защиты информации. Степень защиты данных оказывает непосредственное влияние на надёжность радиосети и ее живучесть, поскольку постороннее вмешательство в работу может существенно снизить эти параметры. Ниже представлена информация о возможностях данных радиосетей противостоять основным угрозам: перехвату данных, несанкционированной работе в составе радиосети и радиоэлектронным помехам[5].

3. Устойчивость радиосети к перехвату данных

На первый взгляд, перехват данных в проводных технологических сетях связи сопряжен с серьезными трудностями. Однако эта задача не так сложна для специалиста, имеющего соответствующую подготовку (подтверждением этому являются многочисленные успешные атаки «хакеров»[6] на информационные системы различных ведомств и организаций). Кабельная сеть, прокладывается внутри здания или комплекса зданий. При этом отдельные сегменты могут укладываться в подвалах зданий, коллекторах, потернах и т. п., не контролируемых службами безопасности, и представлять собой потенциальные точки для несанкционированного подключения. Теоретически любой человек, знающий структуру кабельной системы, может получить доступ к ней в этих точках. После подключения к проводной системе связи получение доступа к информации является делом техники, поскольку во всех открытых проводных сетях используются стандартные протоколы связи и обмена данными, а также серийно выпускаемые и общедоступные программно-технические средства.

Средой передачи данных в стационарных и подвижных радиосетях являются радиоволны, которые могут приниматься любым приемником на относительно большом расстоянии от передатчика. Однако, радиосигналы, передаваемые в радиосетях обмена данными с использованием современного радиотехнического оборудования, не так доступны, как это может показаться на первый взгляд.

Во-первых, для организации перехвата необходимо точно знать номинал рабочей частоты, используемой для обмена данными. При соблюдении пользователями минимальных правил безопасности получение этой информации крайне затруднено. Поскольку передаваемые данные не могут восприниматься на

слух, то при использовании для определения номинала рабочей частоты доступных средств перехвата, например, частотных сканеров, фиксируется только факт передачи сигналов на определенной частоте, которые представляются как набор шумов. Определение принадлежности этих сигналов тому объекту, поиск которого ведется, без доступа к передаваемой информации оказывается практически невозможным.

Во-вторых, оборудование использует специальные схемы модуляции сигнала и собственные преамбулы (структуру пакета данных). На практике это выливается в невозможность получения доступа к собственно передаваемой информации при отсутствии соответствующего приемного оборудования или специальных приборов для анализа сигналов. В отличие от проводных средств связи, распространение радиотехнического оборудования имеет известные ограничения, а все его пользователи регистрируются. В связи с этим вероятность легального приобретения оборудования, которое может использоваться для обеспечения доступа к передаваемой в технологических радиосетях обмена данными информации, практически равна нулю.

В-третьих, в большинстве радиосетей, особенно имеющих топологию типа «звезда», в которых обмен данными производится через базовую станцию, в отдельно взятой точке могут приниматься только данные, передаваемые в одном направлении (от базовой станции к удаленному объекту). Это связано с принципами построения сети, в которой базовая станция разворачивается на возвышенности и имеет высоко подвешенную приемо-передающую антенну, что обеспечивает возможность организации связи со всеми удаленными станциями сети, в то время как удаленные объекты такой возможности не имеют. Для организации перехвата используемое для него оборудование необходимо разместить на такой же выгодной позиции, что в большинстве случаев оказывается невозможным. В противном случае обеспечивается перехват только данных от базовой станции, которые, в большинстве стационарных технологических радиосетей представляют наименьший с точки зрения перехвата интерес (например, запросы, которые дают минимальное представление о работе информационной системы). На практике надёжный перехват может производиться только спутниковыми средствами, но для защиты от таких профессиональных средств используются профессиональные же средства противодействия.

И наконец, в отличие от проводных сетей обмена данными, где кабельная инфраструктура и аппаратура для ретрансляции сигналов распределены по всей территории полигона, радиооборудование передачи данных может быть полностью развернуто в охраняемых помещениях, физический доступ в которые строго ограничен.

Совокупность всех перечисленных выше качеств делает полигонные технологические радиосети обмена данными более безопасными по сравнению с проводными сетями связи и обмена данными в части перехвата информации.

2. Устойчивость к несанкционированному подключению

При подключении к сети обмена данными обычно ставится целью получение доступа для работы в составе информационной системы или «просмотру» передаваемых данных. Для решения этой задачи требуется соответствующий терминал, поддерживающий используемые в сети обмена данными протоколы. Такой терминал может быть легко реализован на базе современного компьютера, но решение второй части задачи представляется не таким простым.

Перечисленные выше трудности, возникающие при организации перехвата, встают и при попытке получить доступ к работе в составе сети обмена данными. Кратко описанные ниже свойства применяемых протоколов связи и обмена данными в равной степени относятся к радио и проводным сетям и характеризуют их способности по обеспечению безопасности информации.

Часть технологических радиосетей обмена данными (в первую очередь, стационарных) использует протоколы «опроса», в которых заложены определенные возможности по обеспечению безопасности. Чтобы терминал пользователя распознавался информационной системой, он должен быть внесен в «опросную таблицу», которая ведется и поддерживается на центральном компьютере. Несмотря на то, что система может самостоятельно распознавать новые терминалы и автоматически вносить их в таблицу, содержание таблицы постоянно контролируется администратором сети, который может локализовать нового пользователя, получившего доступ к сети, и предпринять соответствующие меры по исключению возможности его работы в составе информационной системы. Если терминал не будет внесен в таблицу, он не сможет работать в составе сети.

Значительная часть технологических радиосетей используется для обслуживания строго определенного количества терминалов, поэтому появление в их составе новых терминалов вообще не предусматривается.

Возможно, что профессиональный «крэкер»[7] или «хакер» сможет перепрограммировать компьютер таким образом, чтобы получать данные без внесения дополнительного адреса в «опросную таблицу», однако в этом случае он не сможет передавать свои данные в центральный компьютер (что в большинстве случаев является основной целью).

Попытки работы через технологическую радиосеть обмена данными под «прикрытием» другого терминала за счет дублирования его идентификационного номера приводят к генерации некорректных данных и подтверждений, получаемых центральным компьютером. Этот факт незамедлительно привлечет внимание администратора сети. На данном этапе достаточно просто выявить попытку получения несанкционированного доступа к работе в сети и предпринять соответствующие меры для предоставления контролируемой работы или предотвращения доступа к информационной системе. Поскольку основным условием успешного проникновения в сеть является скрытность, уже сам факт выявления попытки несанкционированного доступа делает его дальнейшие действия бессмысленными.

На практике выявить и локализовать несанкционированную работу в технологической радиосети обмена данными намного проще, чем в проводной системе связи. В случае предоставления злоумышленнику возможности продолжения контролируемой работы в сети излучаемые его приемопередатчиком сигналы при посылке запросов и подтверждении приёма сообщений могут быть легко запеленгованы (а поскольку работа в сети управляется с базовой станции администратором, последний может инициировать работу передатчика злоумышленника с необходимой периодичностью), что существенно проще, чем определить точку подключения к проводной сети обмена данными.

3. Устойчивость к подавлению и воздействию помех

Подавление или намеренная постановка помех работе радиосети задача существенно более сложная, чем физическое нарушение соединения в проводной системе, и для большинства технологических радиосетей маловероятна.

Подверженность радиосигналов воздействию помех и возможность их подавления являются непреложным фактом. Однако для выполнения этой задачи необходимо знать номинал рабочей частоты радиосети обмена данными, установить который не так просто, поскольку передача ведется коротким сеансами. Факт появления помех немедленно выявляется администратором радиосети, а источник излучения становится объектом пеленгования и локализации, в том числе, при поддержке соответствующих организаций, контролирующих использование радиочастотного спектра. Кроме того, в некоторых радиомодемах применяются встроенные средства помехоустойчивого кодирования, обеспечивающие устойчивую работу в условиях помех.

Поэтому на практике оказывается гораздо проще незаметно перекусить кусачками пару проводов, чем поставить помеху радиосистеме, используя сложное и дорогостоящее специализированное оборудование, серьезно рискуя при этом быть пойманным. Работа кусачками займет не более 30 секунд, а установка и использование специального оборудования радиопротиводействия требует времени и крупных финансовых затрат, но при этом его воздействие не может быть продолжительным.

(Продолжение следует).

Сноски

1. **Полигон** − участок суши или моря, предназначенный для испытаний различных видов оружия, боевых средств и техники, а также для боевой подготовки войск. П. по назначению делятся на научно-исследовательские, испытательные (ракетные, торпедные, артиллерийские, танковые, авиационные, минные, зенитные, инженерные и др.), заводские (для проверки качества изготовленного вооружения, его пристрелки, отладки) и учебные, на которых проводятся боевые и учебные стрельбы, бомбометания, торпедометания, а также различные учения войск. В зависимости от назначения П. оборудуются наблюдательными пунктами, мишенными установками, блиндажами, укрытиями, средствами связи, снабжаются контрольно-измерительными приборами, транспортными средствами и др. *Большая советская энциклопедия.* ↩
2. **Технологическая сеть связи** (англ. private network, прежнее название «ведомственная», или «корпоративная») предназначена для обеспечения производственной деятельности организаций, управления технологическими процессами в производстве. Технологии и средства связи, применяемые для создания технологических сетей связи, а также принципы их построения устанавливаются собственниками или иными владельцами этих сетей (Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ). ↩
3. **Капу́стин Яр** − ракетный полигон в северо-западной части Астраханской области России. Официальное название: 4-й государственный центральный межвидовой полигон Российской Федерации (4 ГЦМП). www.ru.wikipedia.org. ↩
4. **Ультракоро́ткие во́лны (УКВ)** − традиционное в СССР название диапазона радиоволн, объединяющего метровые, дециметровые, сантиметровые и миллиметровые волны (или диапазоны очень высоких частот − ОВЧ, ультравысоких частот − УВЧ, сверхвысоких частот − СВЧ и крайне высоких частот − КВЧ). То есть это все радиоволны, длина которых менее 10 м (0,1-10 м или 30-3000 МГц), − такая классификация сложилась в отечественной учебной и технической литературе. ↩
5. Вопросы противодействия профессиональным средствам радиоэлектронной борьбы и радиоэлектронного подавления в настоящей статье не рассматриваются. ↩
6. **Ха́кер** (от англ. *hack* - разрубать) − особый тип компьютерных специалистов. Компьютерные взломщики, осуществляющие неправомерный доступ к компьютерам и информации. ↩
7. **Крэкер** (англ. *cracker*) - тип компьютерного взломщика: человек, взламывающий системы защит информационных систем или создающий программные средства для взлома систем защит. Вне профессиональной среды применяется общий термин «компьютерный взломщик» или чаще «хакер», что также часто не является правильным. В абсолютном

большинстве случаев «крэкер» не располагает исходным кодом программы, поэтому программа изучается связкой дизассемблера и отладчика с применением специальных утилит. ↩