Безопасность специальных информационных систем

Колыбельников А. И.

2019

Оглавление

Перечень сокращений

Сокращение	Полное наименование
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
АСУ ТП	Автоматизированные системы управления технологическим процессом
ИБ	Информационная безопасность
ИС	Информационные системы
ИТ	Информационные технологии
КИКС	Корпоративная Информационно-Картографическая Система
ККС	Корпоративная компьютерная сеть
КПП	Контрольно-пропускной пункт
КСМД	Клиент Системы Массового Доступа
ЛВС	Локальная вычислительная сеть
МЭ	Межсетевой экран
НПС	Насосная перекачивающая станция
НСД	Несанкционированный доступ
ООБ	Отдел обеспечения безопасности
ОС	Операционная система
ПЛК	Комплекс программируемых логических контроллеров
ПМВ	Программно-математическое воздействие
ПО	Программное обеспечение
ППО	Прикладное программное обеспечение
РД	Руководящий документ
РДП	Районный диспетчерский пункт
САЗ	Средства анализа защищенности
САТС	Служба автоматизации телемеханики и связи
СЗИ	Средство защиты информации
СКУД	Система контроля и управления доступом
СОВ	Средства обнаружения вторжений
ССИТ	Служба сервиса и информационных технологий
СУБД	Система управления базами данных
ТП	Технологический процесс
ТЭЦ	Теплоэлектроцентраль
УЗ	Учетная запись
ЦДП	Центральный диспетчерский пункт
ЦО	Центральный офис
ACL	Access Control List (список контроля доступа)
DMZ	Демилитаризованная зона
IDS	Intrusion Detection System (система обнаружения вторжений, СОВ)
IP	Internet Protocol (межсетевой протокол)
LDAP	Lightweight Directory Access Protocol (облегчённый протокол доступа к каталогам)
OPC	OLE for Process Control (семейство программных технологий, предоставляющих единый интерфейс для управления объектами автоматизации и технологическими процессами)
VLAN	Virtual Local Area Network (виртуальная локальная компьютерная сеть)
VPN	Virtual Private Network (виртуальная частная сеть)

ВВЕДЕНИЕ

Информационные системы специального назначения давно и прочно вошли в жизнь каждого обывателя. Зачастую, мы их просто не замечаем в повседневной жизни, ведь к этому классу можно отнести, как транспортную систему управления дорожным движением на Московской кольцевой автодороге, так и автоматизированную систему управления технологическим процессом (АСУ ТП) на соседней теплоэлектростанции.

Ранее, эти системы не вызывали столь пристального внимания со стороны хакеров и-экспертов по информационной безопасности. Такое отношение было вызвано изолированностью этих сетей от сетей общественного пользования. Поэтому их недостатки при создании и проектировании компенсировались их закрытостью и ограничением доступа со стороны большинства любителей похулиганить в информационных системах в лице излишне любознательных или нерадивых сотрудников.

Сейчас, когда, многие из информационных систем специального назначения обмениваются информацией через интернет, и предоставляют возможность удаленного доступа к системе управления – такой подход подвергает их риску перехвата управления со стороны злоумышленников.

Иллюстрацией серьезности этих рисков могут служить результаты работы поисковой системы Shodan (http://www.shodanhq.com/), в которых можно отыскать интерфейсы удаленной работы различных корпоративных систем. Многие из найденных в этом сервисе серверов можно назвать критически важными не только для работы отдельной компании, но и для нормальной жизни государств, если рассматривать энергетические системы и объекты атомной энергетики. Они могут быть использованы в процессе информационного противоборства.

Ключевая система информационной инфраструктуры (КСИИ) - это информационно-управляющая или информационно-телекоммуникационная система, в которой сосредоточено управление критически важным объектом (процессом), или информационное обеспечение управления таким объектом (процессом), или официальное информирование граждан, и в результате деструктивных информационных воздействий на которую может сложиться чрезвычайная ситуация, или будут нарушены выполняемые системой функции управления со значительными негативными последствиями.

К ключевым информационным системам можно отнести все действующие информационные системы транспорта, энергетики, связи, добычи полезных ископаемых, производства, государственного управления и средств массовой информации.

В этой книге подробно рассматриваются вопросы безопасности следующих систем:

1. Автоматизированные системы управления технологическим процессом;
2. Системы управления сетями связи

Такой выбор систем для анализа обусловлен тем, что в части систем энергетики, добычи полезных ископаемых и управления производством используются схожие системы управления технологическим процессом с одинаковыми протоколами передачи информации, что подразумевает схожие методы и подходы для их атаки и построения систем защиты информации.

Автоматизированные системы управления технологическим процессом

С точки зрения информационных технологией, автоматические системы управления технологическим процессом (АСУ ТП) – многокомпонентная сетевая распределенная система, предназначенная для управления различными производственными процессами. С точки зрения хакеров эти системы интересны тем, что, нарушив их работу можно вызвать сбой в работе производственной линии[1]. В случае, если в процессе производства используются радиоактивные, токсические или взрывоопасные вещества подобный сбой может привести к катастрофе техногенного характера.

С точки зрения производства автоматизированная система управления технологическим процессом (АСУ ТП) - комплекс программных и технических средств, предназначенный для автоматизации управления технологическим оборудованием на предприятиях. Под АСУ ТП обычно понимается комплексное решение, обеспечивающее автоматизацию основных технологических операций на производстве в целом или каком-то его участке, выпускающем относительно завершенный продукт.

В английской литературе для обозначения АСУ ТП обычно используются термины, Industrial Control System, Process Control Systems или Automatic Control Systems.

В зарубежных источниках можно встретить следующую классификацию АСУ ТП, в соответствие с которой все АСУ ТП делятся на три класса:

SCADA (Supervisory Control and Data Acquisition)[2] - этот термин можно перевести как “система телемеханики”, “система телеметрии” или “система диспетчерского управления”. Предназначение этой системы - контроль и мониторинг объектов с участием диспетчера. Термин

[1]Ю.Н. Федоров Справочник инженера по АСУТП: проектирование и разработка М.: 2008
[2] Boys, Walt "Back to Basics: SCADA". Automation TV: Control Global - Control Design. 2009.

SCADA часто используется в более узком смысле: часто так называется программный пакет визуализации технологического процесса. Однако в данном разделе под словом SCADA следует понимать целый класс систем управления. Для оценки уязвимости SCADA системы ведущие производители систем управления информационной безопасности (SIEM) даже выпускают отдельные продукты в своем составе.

Существует еще один термин в англоязычной литературе PLC (Programmable Logic Controller)[3] - программируемый логический контроллер (или сокращенно ПЛК). Под термином ПЛК часто подразумевается аппаратный модуль для реализации алгоритмов автоматизированного управления. Тем не менее, термин ПЛК имеет и более общее значение и часто используется для обозначения целого класса систем.

Типовые задачи систем PLC:

1. Управление конвейерными производствами;
2. Управление робототехникой;
3. Высокоскоростное управление приводами,
4. Управление позиционирующими устройствами;
5. Сигнализация, оповещение;
6. Управление комплектными технологическими машинами.

DCS (Distributed Control System) - распределенная система управления (РСУ). РСУ, как правило, применяются для управления непрерывными технологическими процессами. Для РСУ отказ, а соответственно и останов технологического процесса, недопустим. Высокая отказоустойчивость достигается путем резервирования аппаратных и программных компонентов системы, использования компонентов повышенной надежности, внедрения развитых средств диагностики, а также за счет технического обслуживания и непрерывного контроля со стороны человека.

Взаимосвязь этих составных частей АСУ ТП приведена на рисунке ниже.

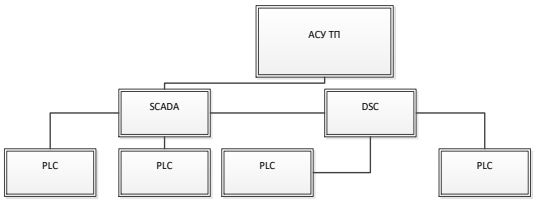

Рисунок 1 Взаимосвязь компонентов АСУ ТП

[3] E. A. Parr, *Industrial Control Handbook*, Industrial Press Inc., 1999 ISBN 0-8311-3085-7

Специальные технические средства защиты информации (СТС) программные и программно-аппаратные комплексы, предназначенные для защиты информации в информационных системах.

Методика анализа защищенности (МОЗ) [4]– алгоритм действий участников процесса защиты информации и использования ими технических средств.

Протокол передачи данных — стандарт, описывающий правила взаимодействия функциональных блоков при передаче данных.

Уязвимость (англ. vulnerability) - могут появляться в результате ошибок программирования и проектирования, некорректных настроек приложений и общесистемного ПО (ОС, СУБД, средств виртуализации, сетевых компонентов), отсутствия, либо неправильной настройки дополнительных средств защиты (межсетевых экранов, антивирусов). Обычно уязвимость позволяет атакующему «обмануть» приложение — заставить его совершить действие, на которое у того не должно быть прав. Это делается путем внедрения каким-либо образом в программу данных или кода в такие места, что программа воспримет их как «свои». Некоторые уязвимости появляются из-за недостаточной проверки данных, вводимых пользователем, и позволяют вставить в интерпретируемый код произвольные команды (SQL-инъекция, XSS, SiXSS). Другие уязвимости появляются из-за более сложных проблем, таких как запись данных в буфер без проверки его границ (переполнение буфера).

Оценка защищенности объектов в критических инфраструктурах осуществляется на основе действующих стандартов по безопасности в системах управления безопасностью с поддержкой архитектуры SCADA, более того за рубежом такие стандарты устанавливаются регулятором в этой области - The North American Electric Reliability Corporation (NERC). В нашей стране действующего единого отраслевого стандарта по безопасности объектов в архитектуре SCADA пока нет как такового. Для примера есть стандарты настройки и конфигурирования информационных систем, описанных в документах Министерства энергетики США на основе рекомендаций производителей оборудования, опубликованных в проекте Digital Bond’s. Что-то подобное по оценке состояния информационной безопасности существует и в атомной отрасли России, где стандарты создания инфраструктуры разработки атомных станций описаны в требованиях регулятора. Но хорошо, когда эти требования подтверждаются реально действующими продуктами и стандартами по безопасной конфигурации устройств. За рубежом таким примером настроек оборудования является стандарт NERC CIP-007 R8.

[4]Зегжда Д.П., Калинин М.О. Методика анализа защищенности ГОУ «СПбГТУ» 2002

Оценка защищенности[5] – это процесс идентификации уязвимостей в исследуемой системе, проводимый как SIEM системой так отдельно стоящим рабочим местом со сканером безопасности. Поиск уязвимостей – часть мероприятий по анализу защищенности информационной структуры, еще необходимо вести сбор логов с промышленных систем и оценивать аномальные события доступа в систему – ведь такие ошибки несанкционированного доступа могут быть следствием ошибок проектирования, реализации или настройки. Как правило, в ходе оценки защищенности сверяются данные с результатами сбора логов в подсистемах авторизации к объектам инфраструктуры и предлагаются варианты устранения найденных уязвимостей путем, повторной проверки системы в целях снижения вероятности успешных атак в дальнейшем. Такие SIEM системы в настоящее время существуют только у потенциального противника и необходимо вести направление в разработке данных систем в России.

Ниже представлена схема информационной структуры АСУ в классической архитектуре SCADA:

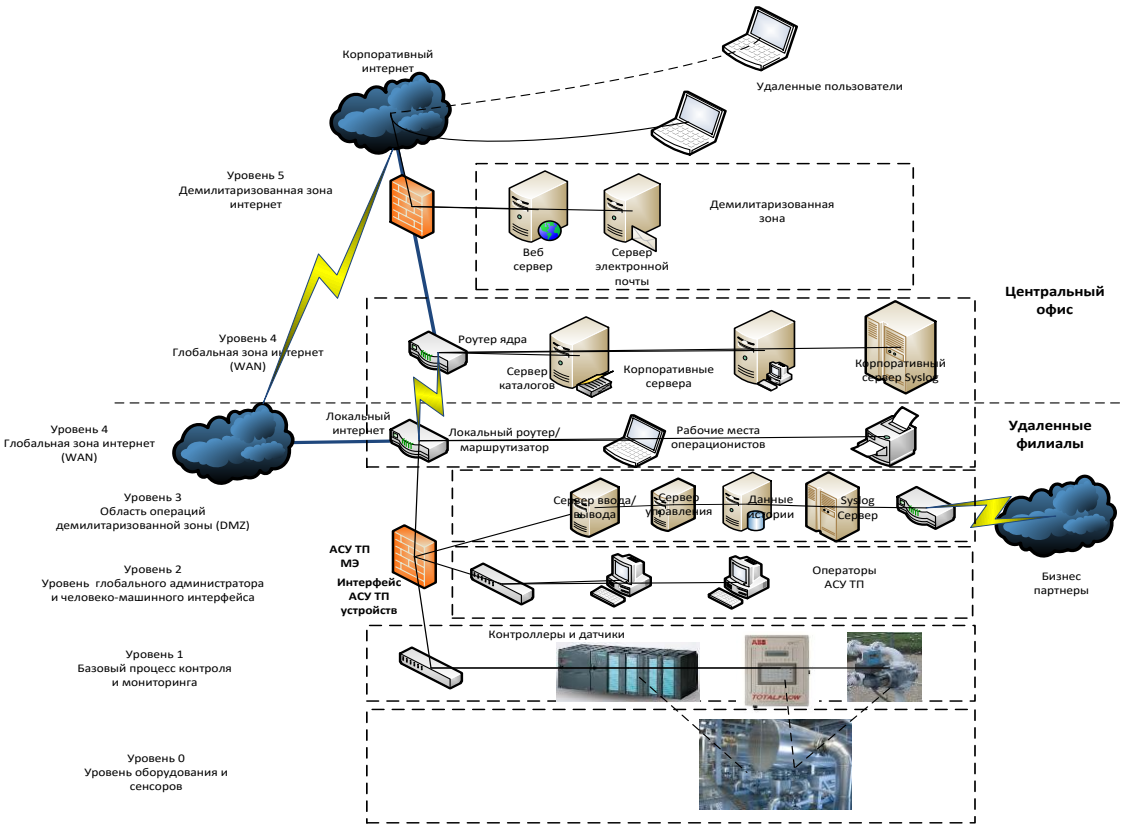

Рисунок 2 Типовая схема АСУ ТП

В общем виде АСУ ТП (ICS) содержит следующие ключевые компоненты:

Контур контроля – состоит из измерительных датчиков, средств управления, таких как PLC, и механизмов, таких как распределительные клапаны, прерыватели, выключатели, двигатели и

[5] ГОСТ Р ИСО/МЭК 15408-2002 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий"

соединения с вариаторами. Управляемые значения переменных передаются от датчиков диспетчеру. Диспетчер интерпретирует сигналы в переменные, оценивает их и корректирует.

Человеко-машинный интерфейс (HMI) – операторы и инженеры используют эти интерфейсы для мониторинга, конфигурирования, установки параметров контроллеров и контроля алгоритмов. Интерфейсы способны отображать как текущую информацию о процессах, так и историческую информацию.

Утилиты диагностики и технической поддержки – используются для предотвращения, идентификации, восстановления после неправильных операций и сбоев.

Сервер контроля - на сервер контроля устанавливается ПО администратора PLC или DSC, которое взаимодействует с устройствами нижнего уровня. Этим серверам подчиняются модули контроля, при помощи сети ICS.

SCADA Server or Master Terminal Unit (MTU) - устройство, которое выступает в роли главного в сети SCADA, ему подчиняются остальные устройства и контроллеры PLC.

Remote Terminal Unit (RTU). Удаленный узел телеметрии предназначен для получения и накопления данных для системы SCADA. Как правило, имеет радио интерфейс и устанавливается в тех случаях, когда нет возможности подключиться при помощи кабеля. Иногда контроллеры PLC в полевом варианте способном работать в качестве RTU.

Programmable Logic Controller (PLC) – программируемые логические контроллеры маленький индустриальный компьютер первоначально разработанные, чтобы выполнять логические функции, реализованные в виде устройств (реле, выключатели, и механические таймеры/счетчики). В ходе развития контроллеры научились работать со сложными комплексными процессами и сейчас являются частью систем SCADA и DCS. Часть контроллеров были разработаны в «полевом» варианте как контроллеры процессов и RTU. Контроллеры PLC часто используются в окружении SCADA так как дешевы, удобны в конфигурации и очень гибки, в отличии от специально разработанных RTU.

Intelligent Electronic Devices (IED) – «умный» датчик способный собирать данные от окружающих устройств и производить первичную обработку. IED объединяет аналоговый вход, аналоговый выход, может контролировать низкоуровневые устройства, имеет систему связи и программируемую память на одном устройстве. Датчики IEDs используются в SCADA и DCS на локальном уровне.

Хранилище данных – централизованная база данных регистрирующая все события в пределах АСУ ТП (ICS). Информация в нем доступна для получения и анализа.

Сервер ввода/вывода Input/Output (IO) Server - компонент подсистемы контроля, ответственный за сбор, буферизацию и обеспечения доступа к информации, обрабатывает информацию от всех типов датчиков. Может быть расположен на сервере управления или на отдельной аппаратной платформе, этот сервер предназначен для интеграции с человеко-машинным интерфейсом.

Сетевые компоненты

Сети АСУ ТП очень сильно различаются по архитектуре, структуре и протоколам передачи данных, но основное их направление развития – это широкое использование сетей Ethernet, протокола TCP/IP и интеграция с внешними сетями и интернет. Это вызвано необходимостью оперативного управления и оперативной отчетности перед руководством компаний. Ниже приведены сетевые компоненты одинаковые для всех типов сетей АСУ ТП.

Сеть «полевая шина» (Fieldbus Network) - этот тип сетей позволяет подключать датчики и различные устройства к контроллерам PLC и другим типам контроллеров. Позволяет избегать двухточечной проводки от сенсора к контроллеру, который может использовать набор разных протоколов. Сенсоры посылают пакеты в сеть, с уникальным идентификатором сенсора используя его контроллер, производит сортировку пакетов и управляет сенсорами.

Контрольная сеть (Control Network) – позволяет управлять устройствами на низком уровне.

Маршрутизатор - коммуникационное устройство, которое передает сообщения между двумя сетями. Использование для маршрутизаторов включает соединение LAN к WAN и подключение MTUs и RTUs к интернету для связи со SCADA.

Межсетевой экран - защищает устройства, в сети контролируя и управляя передачей пакетов. Использует для этого предопределенную политику фильтрации.

Модемы – устройства для модуляции и демодуляции сигнала ИТ – сетей в сигнал телефонной сети и обратно. Часто используются для связи с удаленными компонентами SCADA.

Точки удаленного доступа – позволяют получить удаленный доступ через интернет для управления и контроля АСУ ТП.

Протоколы обмена данными и управления в АСУ ТП

DNP3

Distributed Network Protocol — (стандарт IEEE Std 1815-2010) это протокол передачи данных, используемый для связи между компонентами АСУ ТП[6]. Был разработан для удобного

[6] IEEE Std 1815™-2012 (Revision of IEEE Std 1815-2010) IEEE Standard for Electric Power Systems Communications— Distributed Network Protocol (DNP3)

взаимодействия между различными типами устройств и систем управления. Может применяться на различных уровнях АСУ ТП.

Протокол DNP3 работает на трех уровнях сетевой модели OSI: прикладном (оперирует объектами основных типов данных), канальном (предоставляет несколько способов извлечения данных) и физическом (в большинстве случаев используются интерфейсы RS-232 и RS-485).

Каждое устройство имеет свой уникальный адрес для данной сети, представленный в виде целого числа от 1 до 65520.

EtherCAT

Протокол EtherCAT[7] — стандарт промышленной сети, относимый к семейству Industrial Ethernet и технологиям, используемым для распределенного управления в режиме реального времени. Стандарт протокола EtherCAT разработан компанией Beckhoff, целью разработки протокола было использование технологии Ethernet для автоматизации приложений, которые требуют частого обновления времени, также называемым временем цикла, с низким дрожанием связи и низкими затратами на аппаратное обеспечение. Пакеты EtherCAT пропускаются внутри стандартного фрейма Ethernet.

Управляемые EtherCAT устройства не занимаются приёмом и отправкой пакетов в классическом смысле слова. Вместо этого, каждая полученная дейтаграмма считывается «на лету» одновременно с отправкой дальше. Вставка данных происходит сходным образом. За счёт такого подхода удается добиться малого времени обработки дейтаграммы. Все устройства в сети адресуется одной дейтаграммой, которая последовательно обрабатывается каждым устройством.

Спецификация протокола EtherCAT доступна только членам организации, что значительно удорожает введение устройств EtherCAT в системы диспетчеризации. Протокол EtherCAT оперирует пакетами, передаваемыми непосредственно внутри стандартного фрейма IEEE 802.3 Ethernet (с применением Ethertype 0x88a4) или внутри датаграммы UDP/IP.

FL-net

Протокол FL-net (OPCN-2) - это результат инициативы по стандартизации JEMA (Japan Electrical Manufacturers Asscociation и прочих органов по стандартизации Японии[8]. FL-net – сеть уровня контроллеров, которая дополняется на уровне оборудования сетью OPCN-1. FL-net основывается на Industrial Ethernet, разработана для связи между контроллерами PLC, CNC или роботизированными контроллерами от различных производителей на базе единого открытого стандарта. Его базовая спецификация является обязательной для участников Japan Automobile

[7] IEC/PAS 62407 (Ed 1.0), *Real-time Ethernet control automation technology (EtherCAT)*
[8] FA Control Network [FL-net (OPCN-2)]-Protocol Specifications

Manufacturers Association (JAMA) для построения систем высокой надежности. Устройства сети FL-net сертифицируются на предмет поддержки стандарта FL-net в независимом комитете Japanese certification committee.

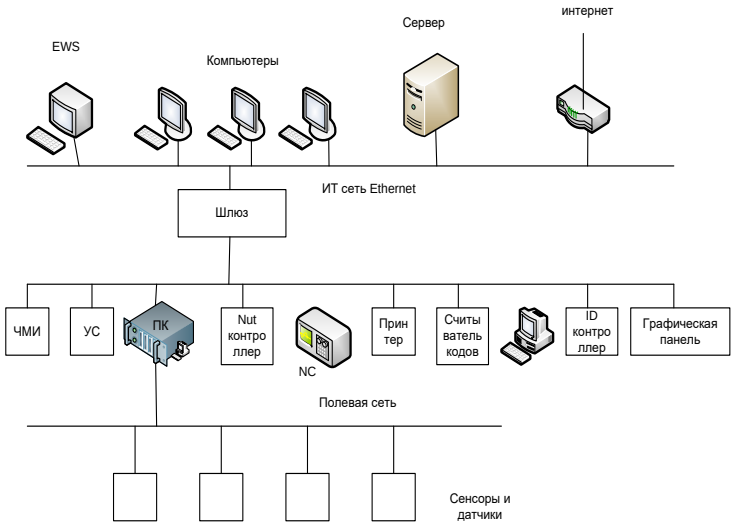

Рисунок 3 Схема работы сети FL-net

Протокол FL-net позволяет объединять в единую сеть компьютеры, контролеры FA, программируемые логические контроллеры (PLC) или компьютеризированные числовые контроллеры (CNC). Данный протокол является открытым, что позволяет использовать оборудование от разных производителей.

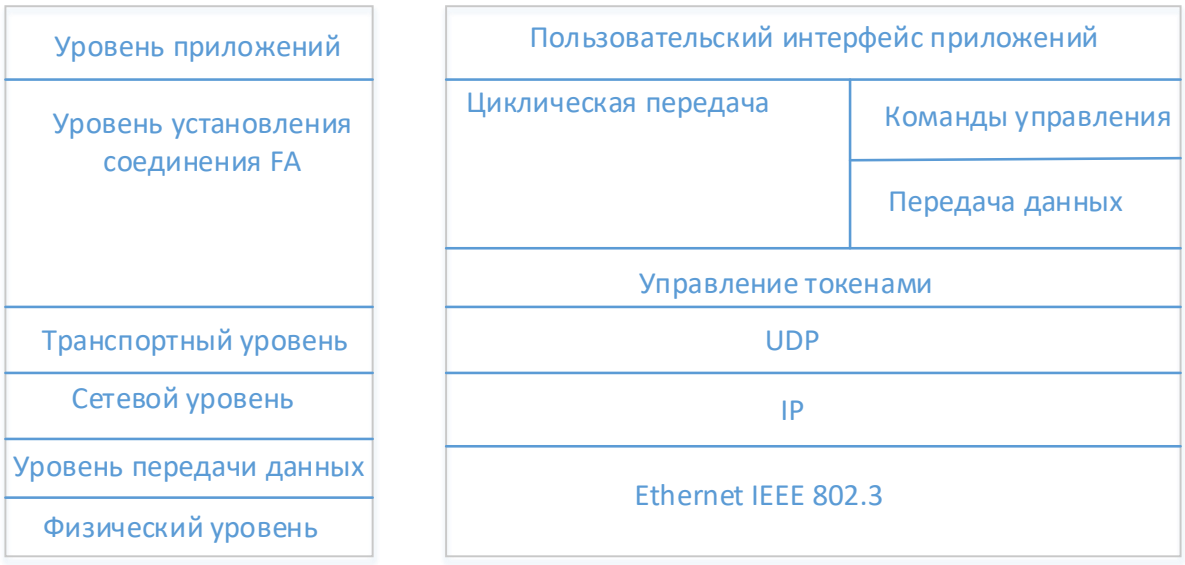

Рисунок 4Соотношение уровней взаимодействия протокола FL-net

В сети FL-net связь между узлами сети устанавливается с использованием номера узла в качестве адреса устройства и общей памяти, называемой регистрами связи. Пакеты передаются в сети циклически от узла к узлу, что не требует установки на узлах дополнительного ПО. Таким образом, передаются команды управления между всеми типами контроллеров и компьютером, дополнительное ПО требуется только в случае передачи данных в этой сети. К сети FL-net можно подключать обычные компьютеры для взаимодействия с контроллерами различных типов,

единственное ограничение, для этого необходима сетевая плата, оснащенная интеллектуальным процессором, в этой роли может выступать обычная сетевая плата для Ethernet, но рекомендуется применение специальных плат для сетей FL-net.

Для сети FL-net обычно устанавливается обычный IP адрес 192.168.250. X, где X меняется в диапазоне от 1 до 250.

Команды управления устройствами сети отличаются от таковых команд в Ethernet и специфицированы в стандарте. Доступ к памяти устройств является открытым и не требует процедуры аутентификации на устройствах, данные передаются в открытом виде, процедур шифрования в протоколе не применяется. Каждый запрос к устройству имеет максимальные привилегии, так как разделения прав доступа не осуществляется.

Foundation Fieldbus HSE

Технология Foundation Fieldbus является цифровым, последовательным, двусторонним протоколом связи, которая служит в качестве базового уровня сети в заводских или фабричных системах автоматизации[9]. Это открытая архитектура, разрабатываются и осуществляются организацией Foundation Fieldbus. Консорциум Fieldbus Foundation является некоммерческой организацией, которая была образована в результате слияния двух других консорциумов, продвигавших протоколы полевых шин, — WorldFIP (North America) и InterOperable Systems Project. В работе Fieldbus Foundation, штаб-квартира которой расположена в городе Остин (штат Техас), участвуют порядка 90% поставщиков аппаратно-программных средств АСУТП на мировой рынок.

Данный интерфейс предназначен для приложений, использующих базовые (контроль) и расширенные (регулирование) возможности дискретного управления, связанные с этими функциями. Foundation Fieldbus технология в основном используется в обрабатывающей промышленности, но в настоящее время она реализуется в электроэнергетике тоже.

Различают две связанные между собой реализации интерфейса Foundation Fieldbus. Они были введены для удовлетворения различных потребностей в среде автоматизированных систем. Эти две реализации используют различные физические среды и скорости передачи и обмена данными.

- Foundation Fieldbus H1 работает на скорости 31,25 кбит/с и обычно соединяется напрямую с полевыми устройствами. Данный интерфейс обеспечивает связь и управление по стандартной витой паре проводов. Foundation Fieldbus H1 в настоящее время является наиболее распространенной в реализации интерфейса.

[9] Fieldbuses for Process Control; Jonas Burge, ISBN 1-55617-760-7

- Foundation Fieldbus HSE (High-speed Ethernet) работает на скорости 100 Мбит/с и, как правило, соединяет входы/выходы подсистем, узлов сети, шлюзов, и полевых устройств с помощью стандартного кабеля Ethernet. Данная реализация этого интерфейса в настоящее время не обеспечивает питание по кабелю, хотя ведутся работы, чтобы решить эту проблему.

Modbus

Modbus — открытый коммуникационный протокол, основанный на архитектуре «клиент-сервер»[10]. Широко применяется в промышленности для организации связи между электронными устройствами. Может использоваться для передачи данных через последовательные линии связи RS-485, RS-422, RS-232, а также сети TCP/IP (Modbus TCP).

Не следует путать MODBUS и MODBUS Plus. MODBUS Plus — проприетарный протокол, принадлежащий Schneider Electric. Физический уровень уникальный, похож на Ethernet 10BASE-T, полудуплекс по одной витой паре, скорость 1 Мбит/с. Транспортный протокол — HDLC, поверх которого специфицировано расширение для передачи MODBUS PDU.

В настоящее время развитием Modbus занимается некоммерческая организация Modbus-IDA.

Стандарты MODBUS состоят из 3 частей:

- Документ Modbus Application Protocol содержит спецификацию прикладного уровня сетевой модели OSI:
    - Элементарный пакет протокола, так называемый PDU (*Protocol Data Unit*), он един для всех физических уровней. PDU упаковывается в индивидуальный пакет для каждого транспорта *application data unit* (ADU).
    - Коды функций и состав PDU для каждого кода.
- Документ Modbus over serial line содержит спецификацию канального и физического уровней сетевой модели OSI для физических уровней RS-485 и RS-232. В принципе, может использоваться любой физический уровень, основанный на асинхронном приемопередатчике.
- Документ MODBUS Messaging on TCP/IP Implementation Guide содержит спецификацию ADU для транспорта через TCP/IP стек.

[10] Modbus for Field Technicians Peter Chipkin 2010

Modbus TCP

Протокол MODBUS TCP/IP базируется на стеке протоколов TCP/IP и прежде всего, предназначен для работы на базе сетей Ethernet[11]. Этот протокол детально описан в спецификациях MODBUS-IDA, согласно которым, коммуникационная система MODBUS TCP/IP может включать в себя различные типы устройств:

- MODBUS TCP/IP Клиенты и Серверы, подключенные к TCP/IP сети;
- межсетевые устройства типа мостов, маршрутизаторов или шлюзов для соединения TCP/IP сети с последовательными линиями подсетей, что позволяет обмениваться данными с MODBUS Serial серверными устройствами.

Таким образом, коммуникационная система MODBUS TCP/IP позволяет обмениваться устройствам не только на сетях со стеком TCP/IP, а также с устройствами на последовательных линиях связи (MODBUS RTU/ASCII или MODBUS+).

OPC US

OPC Unified Architecture (англ. Унифицированная архитектура OPC) — спецификация, определяющая передачу данных и взаимодействие устройств в промышленных сетях[12]. Разработана промышленным консорциумом OPC Foundation и значительно отличается от его предшествующих спецификаций. Этот вариант архитектуры обладает объединённым механизмом адресации и доступа к данным. Получение текущих и архивных значений происходит единообразно, от одного источника. В OPC UA был изменен механизм взаимодействия сервера и клиента, произошел отказ от использования DCOM в пользу XML, что положительно повлияло на безопасность этого протокола, так как сообщения XML проще фильтровать при помощи межсетевых экранов. Протокол использует авторизацию пользователей на базе сертификатов PKI и шифрование передаваемой информации.

Протокол OPC UA состоит из двух подпротоколов, которые с точки зрения приложений и программистов будут отличаться лишь URL:

1. Двоичный протокол

- обеспечивает лучшую производительность, минимальные накладные расходы;
- потребляет минимум ресурсов (не требуются парсер XML, SOAP и HTTP, что важно для встраиваемых устройств);

[11] MODBUS MESSAGING ON TCP/IP IMPLEMENTATION GUIDE 2002
[12] OPC UA 1.02 Part 1: Overview and Concepts

- наилучшая совместимость (двоичный код определён явно и допускает меньшую степень свободы в процессе исполнения в отличие от XML);
- всего один порт TCP (4840) используется для коммуникации и легко может быть туннелирован или пропущен через межсетевой экран.

2. Веб-службы (SOAP)

- легко могут быть использованы, например, из окружения Java или .Net;
- применимы с межсетевыми экранами. Порты 80 (http) и 443 (https) обычно будут использоваться без дополнительных настроек.

Так как имеющийся стек ANSI C поддерживает оба протокола, то ожидается, что большинство конечных продуктов смогут обмениваться информацией по более эффективному двоичному протоколу.

Безопасность унифицированной архитектуры основывается на применении процедур аутентификации и авторизации, шифрования и обеспечения целостности данных при помощи сигнатур. Для этого OPC Foundation ориентировалась на спецификации Web Service Security. Для веб-служб используются WS Secure Conversation и, следовательно, они совместимы с .NET и другими реализациями SOAP. Для двоичного протокола реализованы алгоритмы WS Secure Conversation, которые конвертируются в двоичный эквивалент, в этом случае они называются UA Secure Conversation. Также существует смешанная версия протокола, где код двоичен, но транспортным уровнем является SOAP. Двоичное кодирование всегда требует UA Secure Conversation. При аутентификации используются исключительно сертификаты x509. В результате, можно использовать Public Key Infrastructure (PKI) из Active Directory.

Протокол OPC Unified Architecture позволяет использовать PKI инфраструктуру и протоколы TLS, Kerberos для установления защищенных соединений между всеми узлами сети. Контроллеры, использующие данных протокол способны использовать сертификаты открытых ключей для установления защищенных соединений. В протоколе, также, предусмотрена интеграция с LDAP, что позволяет использовать механизм разделения прав доступа.

PROFIBUS/PROFINET

Протокол PROFINET — является открытым промышленным стандартом для автоматизации Ethernet PROFIBUS & PROFINET International (PI). PROFINET использует TCP / IP и режим реального времени Ethernet[13].

[13] PROFINET технологии и применение 2009

Концепция протокола PROFINET основана на модульной структуре, так что пользователи могут использовать каскадирование функций. Функции этого протокола существенно отличаются в зависимости от типа обмена данными для выполнения очень высоких требований к скорости.

В PROFINET, существует две спецификации протокола - PROFINET CBA и PROFINET IO. PROFINET CBA подходит для компонентов на основе связи через TCP / IP, а PROFINET IO используется для общения в режиме реального времени в модульных инженерных системах. Обе спецификации можно использовать в сети параллельно.

PROFINET IO была разработана для связи реального времени (RT) и изохронного реального времени (IRT) с децентрализованной периферией.

PROFINET CBA и PROFINET IO могут работать в одно и то же время на одной и той же системной шине. Они могут работать по отдельности или в сочетании, так что подсистема ввода-вывода PROFINET выступает как система PROFINET CBA с точки зрения системы.

Модель протокола

В этом протоколе определены три подпротокола разного уровня:

- TCP / IP для PROFINET CBA - включение оборудования с временем реакции в диапазоне от 100 мс.

- RT (Real-Time) протокол PROFINET CBA и PROFINET IO приложений с циклом до 10мс

- IRT (Isochronous Real-Time) для PROFINET IO приложений в приводных системах с циклами меньше, чем 1 мс

Протокол PROFINET может быть записан и отображен с помощью любого анализирующего устройства Ethernet. В текущей версии программы перехвата сетевых пакетов Wireshark / Ethereal способны декодировать части сообщения PROFINET.

Компоненты

Система PROFINET CBA состоит из различных частей, одна часть охватывает все механические, электрические и IT переменные. Компонент может быть создан с помощью стандартных средств программирования. Компонент описывается с помощью PROFINET Component Description (PCD), файлом в формате XML. Инструмент планирования загружает эти описания и активирует логические взаимосвязи между отдельными компонентами, которые будут созданы для осуществления установки.

Эта модель была в значительной степени основана на стандарте IEC 61499.

Основная идея в том, что CBA всей системы автоматизации во многих случаях может быть разделена на автономные операционные подсистемы, тем самым упростив архитектуру сети. Дизайн и функции могут на самом деле оказаться в идентичных или в слегка измененной форме в нескольких системах. Эти компоненты PROFINET, как правило, контролируются управляемым числом входных сигналов. В рамках компонента, программа управления, написанная пользователем, выполняет требуемые функции в рамках компонента и передает соответствующие

выходные сигналы на другой контроллер. Разработка, ведущаяся производителем - независима. Связи на основе компонентов системы только настраиваются, а не программируются. PROFINET CBA (без реального времени) подходит для шин с цикличностью примерно 50 ... 100 мс. Параллельная работа RT канала позволяет для данных циклов быть похожими на PROFINET IO (несколько мс).

AS-Interface

AS-Interface (англ. Actuator Sensor Interface) — интерфейс датчиков и исполнительных устройств[14].

Промышленная сеть, предназначенная для передачи преимущественно дискретных сигналов, используется обычно в машиностроении. Является «открытой» технологией. Спецификация разработана и поддерживается ведущими производителями систем автоматизации (в настоящий момент свыше 100 фирм-участниц). Топология сети — любая. Для подключения датчиков разработан специальный плоский кабель с подключением под прокол изоляции (ножевые клеммы предусмотрены в конструкции модулей ввода-вывода). Версия AS-i 2.11 позволяет передавать аналоговые сигналы. Новейшей версией спецификации является AS-i 3.0.

Существует профиль протокола для систем повышенной безопасности ASi-Safe. Устройства повышенной безопасности подключаются по тому же кабелю и поддерживают уровень безопасности вплоть до SIL (Safety Integrity Level) 3 согласно IEC 61508 и вплоть до Safety Category 4 согласно EN 954-1.

GENIbus

GENIbus (**G**rundfos **E**lectronics **N**etwork **I**ntercommunications **bus**) — промышленная сеть, разработанная Grundfos для управления собственными насосами, моторами и другим подобным оборудованием. Сеть предназначается для управления оборудованием, мониторинга, конфигурации и тестирования.

Физический уровень сети базируется на стандарте RS-485 со скоростью передачи 9600 бод/с. Применение стандарта RS-485 обеспечивает возможность подключения типа шина, а низкая скорость передачи данных обеспечивает возможность передачи информации на большие расстояния.

---

[14] NF EN 50295-1999 Аппаратура коммутационная и механизмы управления низковольтные. Системы взаимодействия между устройством и контроллером. Интерфейс пары датчик-механизм конечного выключателя (AS-i)

Сеть GENIbus использует топологию типа шина, работающую по принципу ведущий-ведомые и поддерживающую подключение до 32 устройств.

Ведущее устройство может передавать сообщения на шину по собственной инициативе. Ведомое устройства только прослушивают шину или отвечают по запросу ведущего устройства.

Ведущее устройство может быть центральным управляющим устройством SCADA-системы, контроллером шины или шлюзом в другую сеть.

Протокол поддерживает возможность работы шины с более чем одним ведущим устройством.

Для управления оборудованием Grundfos через общепромышленные протоколы передачи данных используются интерфейсы CIM или CIU. Модуль CIM представляет собой плату, которая устанавливается внутрь изделия Grundfos на производстве, при пусконаладке или в процессе эксплуатации. Блок CIU представляет собой отдельное изделие, внутри которого размещен модуль CIM и блок питания на напряжение 24-240 В AC DC.

Интерфейсы CIM и CIU выпускаются для следующих промышленных сетей:

- LonWorks - интерфейсы CIM/CIU 100, 110.
- BACnet MS/TP - интерфейсы CIM/CIU 300.
- Profibus DP - интерфейсы CIM/CIU 150, 152.
- PROFINET IO - интерфейсы CIM/CIU 500.
- Modbus RTU - интерфейсы CIM/CIU 200, 202 через проводную сеть, CIM/CIU 250 через сеть GSM.
- Modbus TCP - интерфейсы CIM/CIU 500 через Ethernet, CIM/CIU 250 через GPRS.

Безопасность АСУ - ТП

Обобщая все вышеизложенное, следует отметить, что все рассмотренные протоколы, так или иначе работают с использованием Industrial Ethernet или взаимодействуют с другими сегментами сетей, основанными на использовании TCP/IP. Такой подход в построении промышленных сетей привел к тому, что многие угрозы, характерные для ИТ сетей стали актуальными и для промышленных сетей. Промышленные сети, в свою очередь, оказались к ним не готовы, так как их протоколы, очень часто, не предусматривают использования процедур шифрования, аутентификации, разделения прав доступа и прочих механизмов обеспечения безопасности вычислительных сетей. Такое положение дел возникло исторически, и связано с несколькими причинами:

1. Промышленные сети, до последнего времени, всегда были локальными.

2. Промышленные сети использовали свои, не связанные с TCP/IP протоколы.
3. Промышленные сети ориентированы на взаимодействие в реальном режиме времени, а любые процедуры безопасности вносят задержку в передачу информации.

Этого было достаточно для того, чтобы обеспечить безопасность промышленных сетей на промышленных объектах под управлением АСУ ТП. Но, со временем, подход к построению промышленных сетей изменился. В настоящий момент мы получили большое количество угроз в АСУ ТП, которые крайне сложно парировать без модификации протоколов промышленных сетей производителями.

Механизм атаки на АСУ-ТП

Для того, чтобы успешно атаковать АСУ-ТП хакеру необходимо собрать предварительную информацию об атакуемой сети. Прежде всего, хакера будет интересовать состав и архитектура атакуемой сети, а также, точки подключения данной сети к сети интернет. Информацию о составе сети и архитектуре очень часто можно получить на сайте атакуемой компании или на сайте производителя оборудования АСУ-ТП в виде опубликованных пресс-релизов о внедрении. Кроме того, можно использовать техники социальной инженерии для сбора этой информации непосредственно у специалистов атакуемой компании через социальные сети, сайты трудоустройства, профильные форумы и пр. Поиск точек подключения АСУ-ТП к интернету осуществляется при помощи сканеров информационной безопасности или путем использования поисковика Shoudan.

После того, как была собрана предварительная информация об объекте атаки, необходимо выбрать инструменты, которые позволят эффективно атаковать АСУ-ТП. Поскольку эти сети далеко не всегда используют полный стек протоколов TCP/IP, скорее всего, придется искать специализированные сканеры или отладчики для протоколов АСУ-ТП, так как обычный сетевой сниффер вряд ли сможет разобрать передаваемые по сети пакеты, так как они используют свои форматы сетевых пакетов.

На следующем этапе, ищутся уязвимости ПО и оборудования, имеющего выход в интернет, поиск происходит при помощи сканеров уязвимостей, по собранной информации определяется какими уязвимостями обладают узлы атакуемой сети, что позволяет выбрать конкретный метод атаки сети. На первом этапе целью хакера является получение прав доступа в атакуемую сеть, и лишь потом он будет пытаться получить доступ к сегменту промышленной сети, будь то сеть АСУ-ТП или телеком.

На втором этапе атаку сильно упросит отсутствие в специализированных сетях разделения прав доступа, отсутствие шифрования и аутентификации информации. Чаще всего, для полноценной эксплуатации уязвимостей промышленных сетей хакеру придется собрать информацию и детально разобраться с протоколом этой сети и уже после этого самостоятельно реализовать

перехватчик запросов или вирус для промышленной сети. Такой подход требует высокой квалификации атакующего. Но практически полное отсутствие средств и механизмов защиты промышленных сетей делают описанный подход эффективным.

Описание типовых уязвимостей ключевых систем

Уязвимости АСУ ТП можно разделить на несколько типов, классификация согласно стандарта NIST SP 800-115 приведена в таблицах ниже.

Уязвимости политик и процедур

Уязвимость	**Описание**
Несоответствие политик безопасности	Часто уязвимостью является неправильно настроенная политика информационной безопасности
Отсутствие программы обучения и повышения осведомленности	Для поддержания необходимого уровня безопасности необходима программа постоянного повышения осведомленности персонала и обучения.
Неадекватная архитектура и реализация ИБ	Как правило, инженеры ключевых систем имеют мало опыта в разработке систем безопасности, что приводит к ошибкам проектирования
Недокументированные возможности ИБ	Все процедуры и функции защиты информации созданные в процессе разработки должны быть задокументированы
Отсутствуют или несовершенны инструкции по эксплуатации оборудования	Инструкции по эксплуатации для последней версии оборудования должны быть доступны инженерам и операторам
Нехватка административных механизмов обеспечения безопасности	Администраторы безопасности должны быть ответственны за документирование политик и процедур ИБ
Отсутствие аудита ИБ в ключевых системах	Независимая проверка должна проходить не периодической основе, должны исследоваться вопросы устойчивости к различным атакам.
Нет плана обеспечения непрерывности и восстановления после аварий	Планы обеспечения непрерывности и восстановления должны быть приготовлены и протестированы заранее
Ключевые системы используется без системы	Должна существовать система управления изменениями для всех компонентов ключевых систем

управления изменениями	

Уязвимости платформ

Уязвимость	**Описание**
Отсутствие обновлений для ОС	Для многих ОС которые были сняты с поддержки из-за устаревания появляются новые уязвимости, которые некому устранять обновлениями;
Конфигурации по умолчанию	Использование конфигураций по умолчанию небезопасно, так как в не все запущенные сервисы используются в работе и контролируются
Отсутствие шифрования на мобильных устройствах	Если данные на мобильных устройствах, типа ноутбука, планшета и телефона не шифруются, то они могут быть скомпрометированы при потере носителя данных
Недостатки парольной политики	Парольная политика должна определять требования к длине, сложности и времени действия паролей. Пароль должен использоваться, и система должна требовать ввода пароля при включении, временном блокировании и смене пользователей
Раскрытие важной информации	Пароли должны быть конфиденциальными, чтобы предотвратить несанкционированный доступ. Примеры раскрытия пароля: • Регистрация паролей в простом виде, локальном для системы •Совместное использование паролей к отдельным учетным записям пользователями •Передача паролей противникам через социальный инжиниринг • Отправка паролей, которые не зашифрованы через незащищенный канал связи
Подбор пароля	Пароли, которые были созданы без соблюдения политик безопасности по сложности, длине и времени действия пароля могут быть подобраны с использованием таблиц паролей
Некорректные права доступа	К примеру, по умолчанию назначаются права доступа администратора, назначение недостаточных прав доступа для оператора, которые не позволяют предотвратить и локализовать инциденты в сети
Ошибки в механизмах авторизации	Подобная ситуация может привести к следующим последствиям: отключение оборудования, воровство информации и оборудования,

	поломки оборудования и т.д.
Небезопасный удаленный доступ к ключевым системам	Удаленный доступ, если он предусмотрен, должен быть настроен в защищенном варианте
Подключение узлов сети к двум разным подсетям	Доступ во все подсети должен производиться только через авторизацию и
Недокументированные активы	Должно существовать управление активами, иначе недокументированные активы могут становиться точками взлома сети
Радио и электромагнитные импульсы	Оборудование ключевых систем подвержено воздействию радио- и электромагнитным импульсам, потому необходима защита
Отсутствие резервного питания	Отсутствие резервного электропитания для критических компонентов может привести к авариям и катастрофам в случае отключения электричества на основной магистрали
Потеря контроля окружающей среды	Перегрев окружающей среды может привести к отключению ряда процессоров и вызвать критическую ситуацию в ключевых системах
Недостаточный резерв критических компонентов	Отсутствие резервных мощностей может стать причиной отказа системы в целом

Уязвимости программного обеспечения

Уязвимость	**Описание**
Переполнение буфера	Одна из самых распространенных уязвимостей ПО АСУ ТП, может быть использована для атаки
Установленные средства безопасности не настроены	Установленные и не включенные и ненастроенные системы безопасности бесполезны.
Отказ в обслуживании (DoS)	Программное обеспечение может быть уязвимым для атак подобного типа
Слабое определение недопустимых условий	Некоторые ключевые системы уязвимы для задания недопустимых значений
OLE для управления процессом (OPC)	Без обновлений OPC уязвимо по известным RPC/DCOM

использует процедуры удаленного вызова (RPC) и распределенные компоненты объектной модели (DCOM) Некоторые реализации ключевых систем уязвимы к измененным пакетам	
Использование уязвимых протоколов АСУ ТП	Протоколы Distributed Network Protocol (DNP) 3.0, Modbus, Profibus передают информацию в открытом виде
Отсутствие шифрования	Многие АСУ ТП уязвимы к перехвату информации
Запущены ненужные сервисы	Многие сервисы и процессы запускаются по умолчанию, их нужно отключать.
Ошибки при аутентификации	Неавторизованный доступ к конфигурации ПО и к программным интерфейсам
Не установлена система обнаружение вторжений	Для защиты ключевых систем необходимо иметь систему предотвращения вторжений, ее отсутствие чревато пропуском ряда атак, таких как DoS атаки.
Отсутствие, либо некорректная настройка аудита событий	Система должна позволять провести расследование инцидентов
Инциденты не обнаруживаются	В случае если не установлены агенты системы мониторинга и сенсоры безопасности, часто в системе отсутствует возможность обнаруживать атаки в реальном режиме времени.
Отсутствуют средства антивирусной защиты	Антивирус необходим.

Уязвимости системы защиты от вредоносного ПО

Уязвимость	**Описание**
ПО защиты от вредоносного кода не	Вредоносное ПО может нанести вред оборудованию информации, снизить их скорость работы. Потому необходимо применение

установлено	антивируса.
Антивирус не обновлен до текущей версии	Обновление антивирусных баз необходимо для максимально эффективной работы антивируса иначе будут пропуски
Антивирус реализован без исчерпывающего тестирования	Не протестированный антивирус способен повлиять на бесперебойную работу ключевых систем

Уязвимости сетевых настроек

Уязвимость	**Описание**
Слабая сетевая архитектура	Очень часто, при проектировании АСУ ТП учитываются требования только бизнеса и производства, и игнорируется безопасность
Не используются средства управления потоками данных	Списки листов доступа – очень удобное средство для фильтрации нежелательного трафика.
Плохая конфигурация устройств защиты информации	Использование настроек по умолчанию часто является небезопасным
Конфигурации сетевых устройств не сохраняются в резервный архив	Должна быть процедура быстрого восстановления настроек безопасности после сбоев
Пароль передается в незащищенном виде	Передача незащищенных паролей между компонентами ключевых систем чревата их перехватом
Не определены сроки смены паролей на сетевых устройствах	Пароли не должны быть постоянными, необходимо их менять, что бы окно компрометации системы в случае утери пароля было небольшим.
Применение несоответствующих средств управления доступом	Несанкционированный доступ к сетевым устройствам может привести к выводу сети из строя

Уязвимости сетевого оборудования

Уязвимость	**Описание**

Неадекватная физическая защита сетевого оборудования	Отсутствие физической защиты оборудования приводит к его порче и краже
Небезопасные физические порты	Небезопасный серийный порт, USB или PC/2 может привести к подключению через них зараженных вирусами устройств
Потеря контроля за окружающей средой	Чревато перегревом оборудования и выходом его из строя
Персонал имеет излишний доступ к оборудованию	Широкий доступ к оборудованию чреват широким спектром проблем, от кражи самого оборудования, до перехвата информации.
Нехватка избыточных связей и узлов сети	Нехватка избыточности в сети может привести к выводу сети из строя при отключении критичных узлов

Уязвимости сетевого периметра

Уязвимость	**Описание**
Не контролируется сетевой периметр	Если сетевой периметр четко не определен, то очень сложно обеспечить его безопасность
Некорректно конфигурирован межсетевой экран	Неправильная конфигурация межсетевых экранов может приводить к реализации атак в сети
Контрольная сеть используется для других типов трафика	Сеть контроля и управления предназначена только для этого, нельзя через нее передавать трафик других типов, это сказывается на надежности этой подсети и на возможности заражения
Необходимые службы сети должны располагаться в контрольной сети	Сервисы DNS и DHCP необходимые для работы сети контроля и управления должны быть отделены от аналогичных сервисов в ИТ сети, что бы обеспечить необходимую надежность работы ключевых систем

Уязвимости сетевого мониторинга и сбора журналов событий

Уязвимость	**Описание**
Неправильные логи МЭ и сетевых маршрутизаторов	Без точных журналов безопасности невозможно расследование инцидентов

Нет мониторинга ИБ в сети ключевых систем	Без регулярного контроля ИБ инциденты могут быть не замечены, необходим периодический контроль

Коммуникационные уязвимости

Уязвимость	**Описание**
Нет идентификации в контрольной сети	Возможно наличие не декларированной возможности в ключевых системах для взлома
Использование протоколов с открытой передачей данных	Использование протоколов FTP, Telnet, файловой системы NFS может привести к разглашению информации
Нестандартная или отключенная аутентификация	Многие стандартные протоколы ключевых систем не содержат алгоритмов аутентификации
Нет проверки целостности	Большинство протоколов ключевых систем не позволяют проверять целостность передаваемой информации, что позволяет ее заменить, необходимо использование IPSec и его аналогов

Уязвимости беспроводных подключений

Уязвимость	**Описание**
Недостаточная аутентификация между клиентом и точкой доступа	Нужна сильная аутентификация и подтверждение для пользователей, что точка доступа не является ложной
Слабое шифрование между клиентом и точкой доступа	Необходимо использовать надежные алгоритмы шифрования

Модель нарушителя

Нижеприведённая модель нарушителя

Источник угрозы	**Описание**
Хакеры	Ряд хакеров взламывает системы для повышения самомнения, но большинство из них делает это с деструктивной целью и целью получения выгоды.

Операторы бот-сетей	Хакеры и операторы бот-сетей способны использовать распределенные вредоносные сети для различных типов атак на ключевые системы.
Криминальные группы	Криминальные группы, действуя в собственных интересах и интересах транснациональных компаний, нацелены на системы, в результате взлома которых можно получить финансовую прибыль. Как правило, используется весь инструментарий взлома.
Иностранные разведки	Иностранные разведки разрабатывают и используют средства сбора и анализа информации. Многие из них имеют агрессивные доктрины информационной борьбы и нацелены на нанесение ущерба экономике и сектору ВПК.
Инсайдеры	Сотрудники компании или компании – аутсорсера в случае если они нелояльны работодателю способны нанести существенный ущерб ключевым системам так как обладают доступом и правами для входа в систему.
Фишеры	Phishers - люди или небольшие группы, которые пытаются при помощи ложных ресурсов и фишинговых уловок получить идентификационные данные пластиковых карт и других финансовых инструментов. Могут также использовать спам и шпионящее ПО/вредоносное программное обеспечение.
Спаммеры	Люди или организации, распространяющие ложную информацию, чтобы продать продукты, схемы фишинга поведения, распространяет шпионящее ПО/вредоносное программное обеспечение, или организующие атаки (например, DoS).
Вирусописатели	Люди или организации, намеренно выполняющие атаки на различные объекты. Ряд вирусов Melissa Macro Virus, Explore.Zip червь, CIH (Чернобыль), Nimda, Code Red, Slammer, Stuxnet и Blaster способны нанести вред файлам и жесткому диску.
Террористы	Стремятся уничтожить, вывести из строя, или использовать критические инфраструктуры, чтобы вызвать жертвы среди населения и персонала объектов, причинить вред экономике. Возможно предварительное использование вирусного ПО и атаки на объекты с целью отвлечения внимания от других объектов.
Промышленные шпионы	Нацелены на поиск интеллектуальной собственности и know-how

.

Беспроводные сети

Этот раздел книги посвящен обзору основных современных технологий беспроводных сетей, особое внимание уделено рассмотрению вопросов обеспечения их безопасности, так как именно безопасность является одним из главных сдерживающих факторов развития и использования беспроводных сетей.

Основной акцент сделан на рассмотрение протоколов передачи данных. Поскольку, их реализация для сетевого оборудования является фактором, определяющим качество работы устройства, качество оказываемых услуг и безопасности. Именно поэтому основное внимание в части безопасности средств связи будет уделено именно протоколам передачи данных, несмотря на то, что другие аспекты работы средств связи так же важны. Это вызвано тем, что каналы передачи данных, в которых реализованы эти протоколы, находятся в общедоступной части сети связи и на нее может воздействовать кто угодно. Хотя, так же возможна ситуация, когда проникновение хакеров в сервисную сеть операторов связи производится через ИТ – сеть, но такой подход гораздо сложнее, нежели проникновение напрямую. Это связано с тем, что безопасность ИТ - сети развита гораздо лучше, чем безопасность сервисной сети.

Описание протоколов

Bluetooth

Протокол передачи информации по беспроводному каналу связи Bluetooth был разработан группой компаний Ericsson, IBM, Intel, Toshiba и Nokia. Группа разработки была создана в начале 1998 года. 20 мая 1998 года произошло официальное представление специальной рабочей группы (SIG - Special Interest Group), призванной обеспечить беспрепятственное внедрение технологии, получившей название Bluetooth.[15]

Bluetooth обеспечивает обмен информацией между такими устройствами как карманные и обычные персональные компьютеры, мобильные телефоны, ноутбуки, принтеры, цифровые фотоаппараты, мышки, клавиатуры, джойстики, наушники, гарнитуры на надёжной, недорогой, повсеместно доступной радиочастоте для ближней связи. Bluetooth позволяет этим устройствам сообщаться, когда они находятся в радиусе от 10 до 100 метров друг от друга, даже в разных помещениях.

Поскольку Bluetooth имеет ограниченный радиус действия то он применяется только в ИТ сетях, а в сетях телеком его можно встретить только как дополнительную функцию оборудования.

[15] Bluetooth Core Specification Addendum 4

UWB

Протокол UWB был разработан альянсом компаний WiMedia, в 2007 году этот протокол был утвержден в качестве международного стандарта ISO/IEC 26907[16].

WiMedia UWB является стандартом широкополосной беспроводной связи, действующим на короткие расстояния. Протокол затрагивает аспекты взаимодействия между устройствами на физическом уровне (PHY) и подуровне доступа к среде (MAC). Максимальная скорость передачи данных между устройствами WiMedia UWB составляет 480 Мбит/с (как и у проводного USB), устройства работают в диапазоне частот от 3,1 до 10,6 ГГц. Протокол UWB является конкурирующим решением для протокола Bluetooth.

ZigBee

Протокол ZigBee — это стандарт для недорогих, маломощных беспроводных сетей с ячеистой топологией[17]. Низкая стоимость позволяет широко развернуть технологию для беспроводных приложений контроля и наблюдения, маломощность позволяет сенсорам сети работать долгое время, используя автономные источники питания.

Протокол был разработан альянсом компаний ZigBee. Этот альянс является органом стандартизации, определяющим для ZigBee стандарты высоких уровней, он также публикует профили приложений, что позволяет производителям изначальной комплектации создавать совместимые продукты.

Нижние уровни данного стандарта разработаны IEEE и определяются стандартами IEEE 802.15.4-2006.

Сети ZigBee интересны тем, что их стали все чаще применять в АСУ-ТП и в качестве датчиков систем кондиционирования, пожарных датчиков и прочего аналогичного оборудования. Вывод из строя или некорректные данные, поступающие с этих датчиков, могут стать причиной аварии.

Insteon

Протокол INSTEON – разработан для управления беспроводными устройствами для построения «умного дома», в протоколе имеется обратная совместимость с более старым протоколом X10[18]. Скорость передачи сигнала управления в новом стандарте гораздо выше, есть встроенные средства обнаружения ошибок и повторной передачи сигнала, а для передачи используется гибридный канал – радиосвязь и сеть электропитания. Однако, в отличие от X10, спецификации

---

[16] ISO/IEC 26907 ed2.0 Information technology -- Telecommunications and information exchange between systems -- High-rate ultra-wideband PHY and MAC standard

[17] Zigbee Wireless Networking Drew Gislason, President, San Juan Software, Friday Harbor, WA, USA ISBN: 978-0-7506-8597-9

[18] "INSTEON The Details Darbee, Paul Smarthome Technology, 2010

INSTEON защищены патентами и используются только его разработчиками – компанией Smarthome Technology.

Z-Wave

Ячеистая сеть Z-Wave с функциями самоорганизации и самовосстановления, в сочетании с гибкими инсталляционными процедурами, представляет простое в использовании сетевое решение[19]. Протокол Z-Wave и чип с высокой степенью интеграции обеспечивает невысокую стоимость без компромисса с надежностью или универсальностью. Обеспечивается совместимость приложений и устройств Z-Wave, выпущенных разными производителями.

Z-Wave поддерживает полный спектр устройств – устройства, питающиеся от сети переменного тока, питающиеся от батарей, устройства с фиксированным расположением и перемещаемые устройства, а также устройства, выполняющие роль мостов с другими протоколами.

В технологии Z-Wave узлы делятся на три типа: контроллеры (Controllrs), маршрутизирующие исполнительные механизмы (Routing Slaves) и исполнительные механизмы (Slaves). В реальной сети все типы устройств могут работать в любой комбинации.

Эти сети применяются как в АСУ ТП, так и в ИТ, и в качестве обслуживающего оборудования в телекоме.

ANT

Протокол передачи данных - ANT, был разработан компанией Dynastream Innovations[20].

В первую очередь данный протокол разработан для компактных устройств с автономным питанием (трансиверы, использующие этот протокол, отличаются исключительно малым током потребления) для передачи относительно малых пакетов данных. Протокол позволяет организовывать открытые и частные типы беспроводных сетей, в том числе сложного типа с динамической конфигурацией; он создан на основе технологии PAN (Personal Area Network) и поддерживает слои 1 – 4 стека OSI (Open Systems Interconnection network model). Типичное применение такого протокола – беспроводные датчики.

Несущая частота протокола ANT – 2,4 ГГц, количество частотных каналов при этом равно 125 (шаг 1 МГц в диапазоне 2400...2524 МГц). Скорость передачи данных по радиоканалу (включая протокол) может составлять до 1 Мбит/с.

---

[19] ITU-T G.9959:2012 Узкополосные цифровые приемопередатчики для радиосвязи на короткие расстояния. Спецификации физического уровня и уровня доступа к каналу (MAC)

[20] ANT Message Protocol and Usage, Rev 5.0

RuBEE

RuBee (IEEE P1902.1) - двухсторонний протокол беспроводной связи, который использует длинные сигналы волны (LW) и пакеты данных не более 128 байт в местной регионарной сети[21]. Протокол RUBee подобен протоколам серии IEEE 802, также известным как WiFi (IEEE 802.11), WPAN (IEEE 802.15.4) и Bluetooth (IEEE 802.15.1). RuBee network работает по принципу точка-точка, и является развитием стандартов RFID. RuBee использует низкочастотную несущую (131 килогерц), эта рабочая частота позволяет использовать узлы сети с малым потреблением энергии.

RFID

RFID Radio Frequency IDentification, радиочастотная идентификация появилась более тридцати лет назад[22]. В 1973 году Марио Кардулло и соавторы опубликовали патент US 3713148, описывающий первый пассивный транспондер RFID (радиометку). Развитие и широкое внедрение радиочастотной идентификации долго сдерживалось отсутствием стандартизации. Но в 90-х годах прошлого века Международная Организация Стандартизации (ISO) приняла ряд стандартов в области RFID(серия стандартов ISO 18000-6).

X10

X10 — это международный открытый индустриальный стандарт, применяемый для связи электронных устройств в системах домашней автоматизации[23]. Стандарт X10 определяет методы и протокол передачи сигналов управления электронными модулями, к которым подключены бытовые приборы, с использованием обычной электропроводки или беспроводных каналов.

Стандарт X10 был разработан в 1975 году компанией Pico Electronics (Шотландия) для управления домашними электроприборами. Считается, что это был первый стандарт для домашней автоматизации.

WI-FI

Wi-Fi был создан в 1991 году NCR Corporation/AT&T (впоследствии — Lucent Technologies и Agere Systems) в Нидерландах. *Wireless Fidelity* — «беспроводная точность») — торговая марка Wi-Fi Alliance для беспроводных сетей. Основывается на базе стандарта IEEE 802.11.[24]

Обычно схема Wi-Fi сети содержит не менее одной точки доступа, так называемый режим infrastructure и не менее одного клиента. Также возможно подключение двух клиентов в режиме точка-точка, когда точка доступа не используется, а клиенты соединяются посредством сетевых адаптеров «напрямую». Точка доступа передаёт свой идентификатор сети (SSID) с помощью

---

[21] RuBee™ Visibility Networks IEEE P1902.1 (Pending)

[22] ISO/IEC 18000-6:2010 Information technology -- Radio frequency identification for item management -- Part 6: Parameters for air interface communications at 860 MHz to 960 MHz

[23] Standard and Extended X10 Code Protocol Specification

[24] IEEE Std 802.1X-2004 (revision of IEEE Std 802.1X-2001). Port-based network access control

специальных сигнальных пакетов на скорости 0.1 Мбит/с каждые 100 мс. Поэтому 0.1 Мбит/с — наименьшая скорость передачи данных для Wi-Fi. Зная SSID сети, клиент может выяснить, возможно ли подключение к данной точке доступа. При попадании в зону действия двух точек доступа с идентичными SSID, приёмник может выбирать между ними на основании данных об уровне сигнала.

PDC

PDC (Personal Digital Cellular) – стандарт сотовой связи поколения 2G. Был разработан ассоциацией ARIB (Association of Radio Industries and Business) в апреле 2001 года, используется исключительно на территории Японии[25]. В настоящее, время количество абонентов сотовой связи, работающих на данном стандарте, сократилось до 10 миллионов человек. Притом, что в период максимальной распространенности этого стандарта, количество абонентов достигало 80 миллионов человек. PDC использует частотные каналы по 25 кГц с модуляцией pi/4-DQPSK с тремя временными слотами обеспечивающими передачу со скоростью 11.2 кбит/с или 6 временными слотами со скоростью передачи 5.6 кбит/с.

PDC использует два диапазона частот – 800 МГц и 1,5 ГГц.

IDEN

(Integrated Digital Enhanced Networks) технология для сетей транкинговой и сотовой связи, разработана компании MOTOROLA в 1994 году. Основа технологии iDEN— архитектура GSM, при передаче используют частотные каналы по 25 кГц, при этом для передачи данных используется часть каналов в 20 кГц остальное используется для защиты канала. Протокол получил широкое распространение во всем мире. Диапазон частот - 821-825 MHz.

CDMAOne

Стандарт CDMAOne разработан в 1995 году как технологический стандарт группы ANSI. CDMAOne основан на использовании CDMA (множественного доступа с кодовым разделением)[26].

Система CDMA IS-95 фирмы Qualcomm рассчитана на работу в диапазоне частот 800 МГц, выделенном для сотовых систем стандартов AMPS, N-AMPS и D-AMPS. (Стандарты TIA IS-19, IS-20; IS-54; IS-55, IS-56, IS-88, IS-89, IS-90, (S-553).

Последующее развитие технологии CDMA происходит в рамках технологии CDMA2000. При построении системы мобильной связи на основе технологии CDMA2000 1X первая фаза обеспечивает передачу данных со скоростью до 153 кбит/с, что позволяет предоставлять услуги

[25] STD-27 Personal Digital Cellular Telecommunication System
[26] C. Y. Lin and J. Shieh, “IS-95 North American strandard-a CDMA based digital cellular system”, IEEE Website.

голосовой связи, передачу коротких сообщений, работу с электронной почтой, интернетом, базами данных, передачу данных и неподвижных изображений.

WIMAX

WiMAX (Worldwide Interoperability for Microwave Access) — телекоммуникационная технология, разработанная с целью предоставления универсальной беспроводной связи на больших расстояниях для широкого спектра устройств - от рабочих станций и портативных компьютеров до мобильных телефонов[27]. Основан на стандарте IEEE 802.16, который также называют Wireless MAN.

Название «WiMAX» было создано WiMAX Forum — организацией, которая была основана в июне 2001 года с целью продвижения и развития технологии WiMAX. Форум описывает WiMAX как «основанную на стандарте технологию, предоставляющую высокоскоростной беспроводной доступ к сети, альтернативный выделенным линиям и DSL» Максимальная скорость до 1 Гбит/сек.

GSM

GSM (от названия группы Groupe Spécial Mobile, позже переименован в Global System for Mobile Communications) — глобальный цифровой стандарт для мобильной сотовой связи, с разделением частотного канала по принципу TDMA и средней степенью безопасности[28]. Разработан под эгидой Европейского института стандартизации электросвязи (ETSI) в конце 80-х годов.

Коммерческое использование стандарта началось в середине 1991 г., а к 1993 г. было организовано 36 сетей GSM в 22 странах. В дополнение к европейским государствам стандарт GSM выбрали многие страны Южной Африки, Ближнего и Дальнего Востока, а также Австралия. К началу 1994 г. число абонентов GSM достигло 1.3 миллиона. Термин GSM является сокращением от Global System for Mobile telecommunications – глобальная система мобильных телекоммуникаций.

GSM относится к сетям второго поколения (2 Generation), хотя на 2010 год условно находится в фазе 2,75G благодаря многочисленным расширениям (1G — аналоговая сотовая связь, 2G — цифровая сотовая связь, 3G — широкополосная цифровая сотовая связь, коммутируемая многоцелевыми компьютерными сетями, в том числе Интернет).

Сотовые телефоны выпускаются для 4 диапазонов частот: 850 МГц, 900 МГц, 1800 МГц, 1900 МГц.

---

[27] IEEE 802.16 IEEE Standard for Air Interface for Broadband Wireless Access Systems

28 3GPP TS 45.001 V4.0.0 (2000-09) 3rd Generation Partnership Project Technical Specification Group GERAN Digital cellular telecommunications system (Phase 2+) Physical layer on the radio path General description

GPRS

GPRS (General Packet Radio Service — пакетная радиосвязь общего пользования) — надстройка над технологией мобильной связи GSM, осуществляющая пакетную передачу данных. GPRS позволяет пользователю сети сотовой связи производить обмен данными с другими устройствами в сети GSM и с внешними сетями, в том числе интернет[29].

Передача данных разделяется по направлениям «вниз» (downlink, DL) — от сети к абоненту, и «вверх» (uplink, UL) — от абонента к сети. Мобильные терминалы разделяются на классы по количеству одновременно используемых таймслотов для передачи и приёма данных. Современные телефоны (июнь 2006) поддерживают до 4-х таймслотов одновременно для приёма по линии «вниз» (то есть могут принимать 85 кбит/с по кодовой схеме CS-4), и до 2-х для передачи по линии «вверх» (class 10 или 4+2).

UMTS

UMTS (Universal Mobile Telecommunications System — Универсальная Мобильная Телекоммуникационная Система) — технология сотовой связи, разработана Европейским Институтом Стандартов Телекоммуникаций (ETSI) для внедрения 3G в Европе[30]. В качестве способа передачи данных через воздушное пространство используется технология W-CDMA, стандартизованный в соответствии с проектом 3GPP ответ европейских учёных и производителей на требование IMT-2000, опубликованное Международным союзом электросвязи как набор минимальных критериев сети сотовой связи третьего поколения.

Согласно спецификациям стандарта, UMTS использует следующий спектр частот: 1885 МГц — 2025 МГц для передачи данных в режиме «от мобильного терминала к базовой станции» и 2110 МГц — 2200 МГц для передачи данных в режиме «от станции к терминалу». В США по причине занятости спектра частот в 1900 МГц сетями GSM выделены диапазоны 1710 МГц — 1755 МГц и 2110 МГц — 2155 МГц соответственно. Кроме того, операторы некоторых стран (например, американский AT&T Mobility) дополнительно эксплуатируют полосы частот 850 МГц и 1900 МГц. Далее, правительство Финляндии на законодательном уровне поддерживает развитие сети стандарта UMTS900, покрывающей труднодоступные районы страны и использующей диапазон 900 МГц (в данном проекте участвуют такие компании как Nokia и Elisa).

---

[29] EN 301 349 Digital cellular telecommunications system (Phase 2+) (GSM); General Packet Radio Service (GPRS);

[30] TS 25.10U UMTS Radio Aspects; Channel coding

Безопасность беспроводных сетей

Шифрование

Название технологии	Алгоритмы шифрования	Режимы шифрования	Генерация ключей	Смена ключей
Bluetooth	E0	ECB	Есть	есть
UWB	AES	CBC		
ZigBee	AES	CBC	Нет	есть
Insteon	Rolling code system	Нет	Нет	нет
Z-Wave	3DES только в 100 серии	ECB	Нет	нет
ANT	Нет	Нет	Нет	нет
RuBee	AES			
RFID	Crypto1, DES	ассиметричный	Есть	есть
X10	Нет	Нет	Нет	нет
WI-FI	RC4, AES			TKIP
PDC	A5	Поточное	A8	A8
IDEN				
CDMA	CMEA	ECB	SSD	SSD
WIMAX	3DES, AES	ECB	PKM2	PKM2
GSM	A5 (COMP-128)	Поточное	A8	A8
GPRS	GEA1, GEA2	Поточное	-	-
UMTS	A5 (COMP-128) KASUMI MILENAGE		A8	A8

Стандарт шифрования E0

В стандарте Bluetooth применяется поточный шифр E0, построенный на базе 3 линейных генераторов сдвига. Общая схема шифрования и генерации общего ключа приведена на рис 7. Эта схема применяется Bluetooth в режимах обеспечения безопасности 2 и 3. Данные режимы безопасности применяются в протоколе Bluetooth v2.0 + EDR.

Процедура генерации ключа, приведенная на рис 4, происходит следующим образом:

В протоколе Bluetooth v2.0 + EDR (и более ранних версий) работающих в 2 и 3 режиме безопасности, два устанавливающих соединение устройства одновременно получают одинаковый сеансовый ключ, в том случае если пользователь установил для них одинаковый PIN. Ввод PIN-кода и установка сеансового ключа схематически изображены на рис. 8. Необходимо заметить, что, в случае если PIN- код меньше 16 байтов, тогда BD_ADDR используется как дополнение к значению текущего PIN-кода для генерации сеансового ключа.

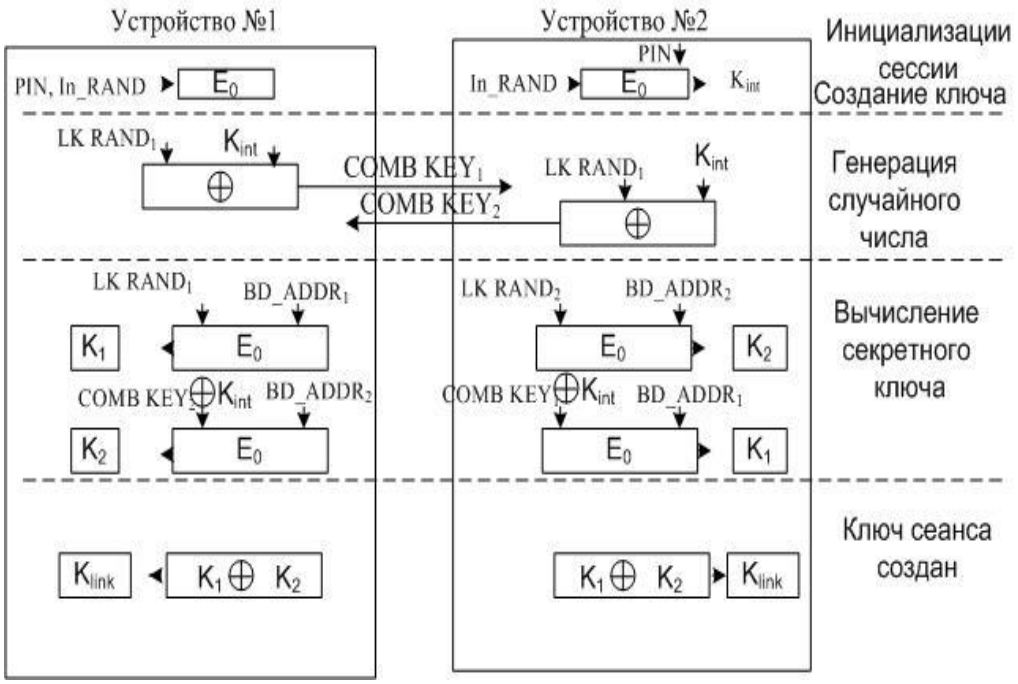

Рисунок 5 Протокол Bluetooth v2.0 + EDR

Рисунок 8. Схема соединения двух устройств Bluetooth для генерации общего ключа

Шифрование

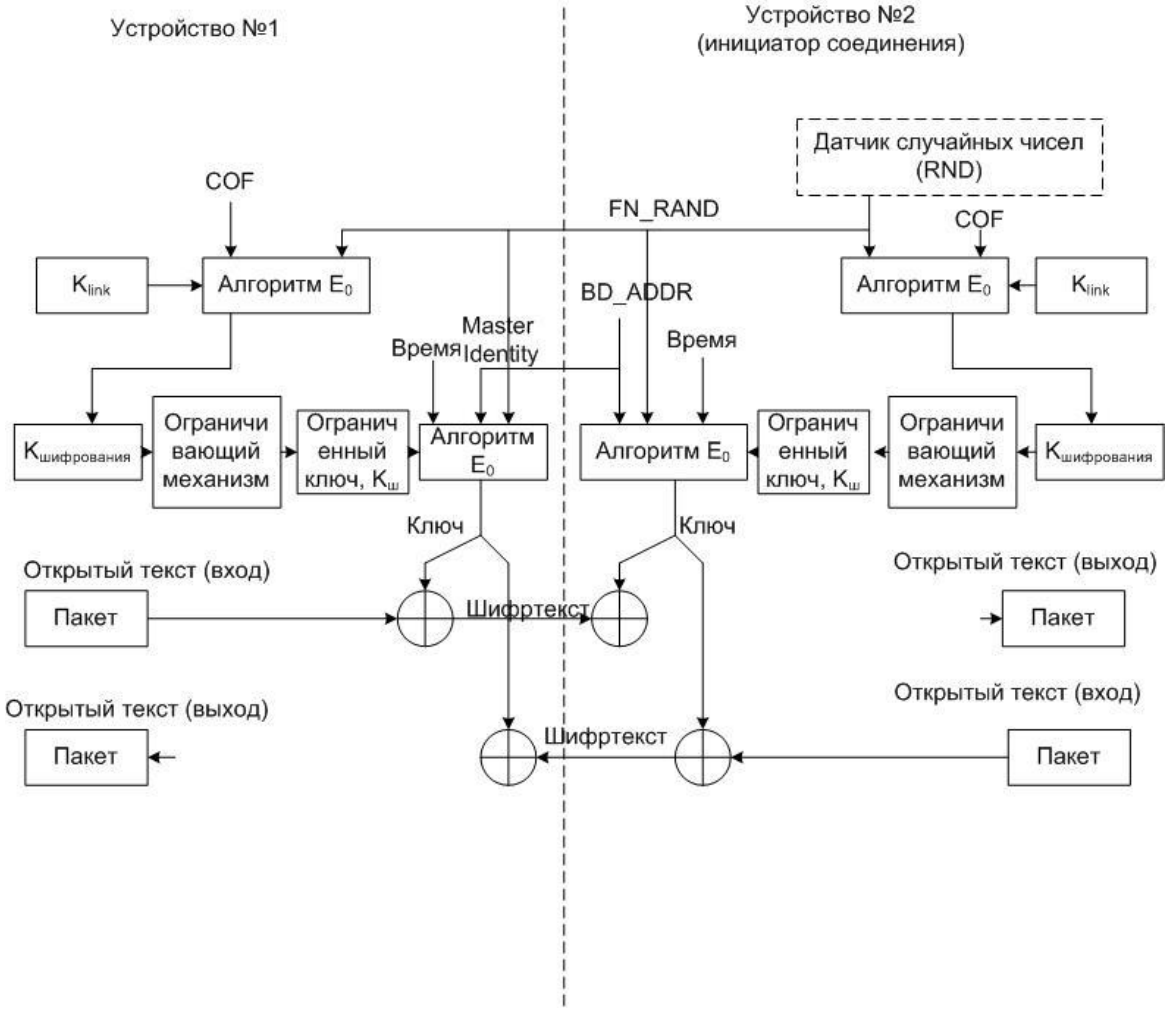

Рисунок 6Алгоритм шифрования E0

Процедура шифрования в протоколе Bluetooth основана на использовании алгоритма потокового шифровая E0. Ключ потока суммируется XOR с битами открытого текста и передается на принимающее устройство. Ключ потока генерируется с использованием криптографического алгоритма на базе линейного рекуррентного регистра (ЛРР). Функция шифрования получает следующие входные данные: главный идентификатор (BD_ADDR), 128- битное случайное число (EN_RAND), номер слота и ключ шифрования, который так же инициализирует ЛРР в случае, если шифрование включено. Номер слота, используемый в потоковом шифре, меняется с каждым пакетом, меняя, таким образом, инициализацию ядра шифра, в то время как другие переменные не меняются.

Ключ шифрования КС генерируется из текущего сеансового ключа и может иметь длину от 8 до 128 бит. Установление размера ключа происходит в ходе установления сеанса шифрования между устройствами. Начальный размер ключа вносится в устройство производителем и не всегда он указан максимального размера.

Следует отметить, что алгоритм E0 не сертифицирован FIPS как национальный стандарт.

В настоящее время существует теоретическая оценка стойкости данного алгоритма к атаке со знанием открытого текста за 238 переборов, в то время как атака грубой силы требует перебрать 2128 возможных ключей.

Стандарт шифрования Elliptic Curve Diffie Hellman (ECDH)

В 4 режиме обеспечения безопасности протокола Bluetooth v2.1 + EDR используется пара ключей безопасного простого сопряжения (Secure Simple Pairing). Эта пара ключей является ключами алгоритма ассиметричного шифрования Диффи-Хеллмана на эллиптических кривых.

Взаимодействие между двумя абонентами с использованием ключей SSP приведено на рис. 10.

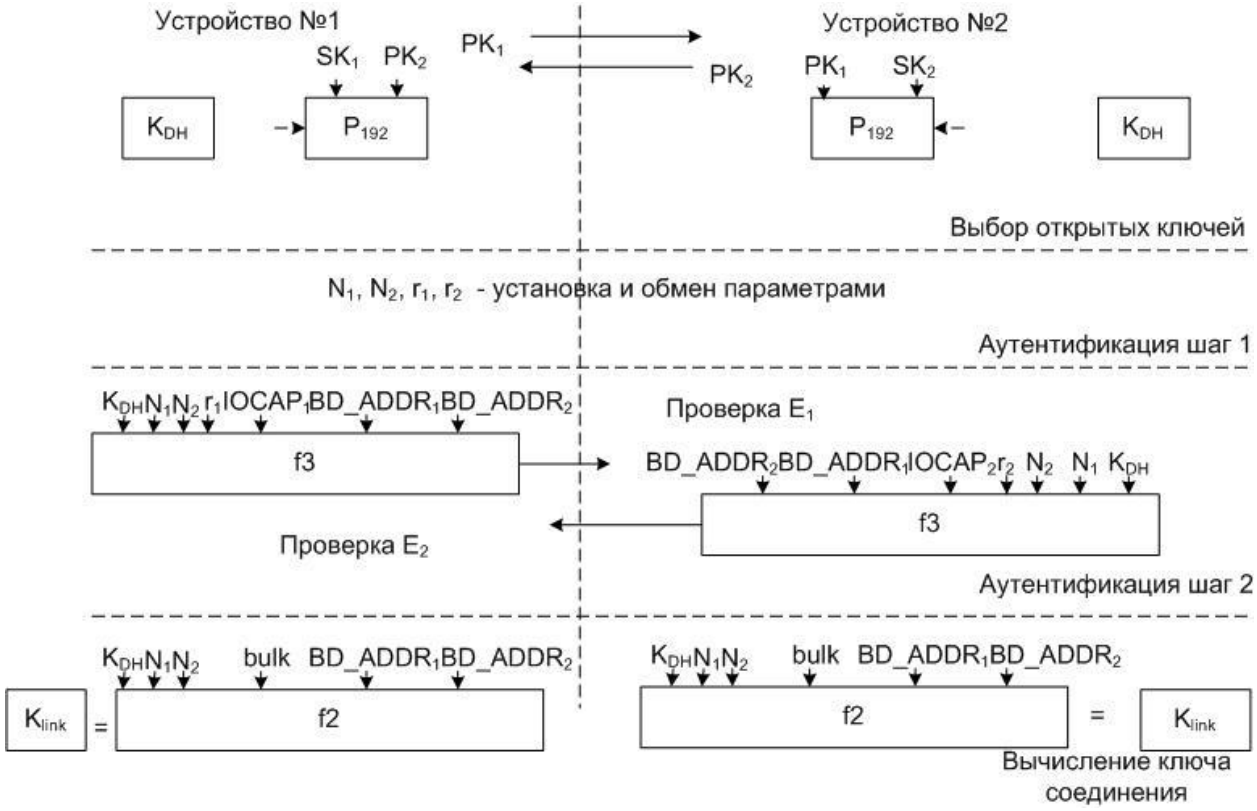

Рисунок 7 Взаимодействие между абонентами при помощи ключей SSP

Алгоритм шифрования A5

Поток данных (передаваемый на DCCH и TCH) шифруется побитно (потоковым шифром) то есть, поток данных получаемых по радиоканалу от пользователя и поток битов ключа, сгенерированный алгоритмом A5 суммируются. Ключ шифрования - K_c.

Для многоканальных конфигураций, например, SCSD, используются разные ключи для разных каналов. Для канала n создается алгоритмом A5 ключ Kcn, при этом ключ Kcn является производным от ключа Kc, вычисление первого ключа из второго производятся следующим образом:

Пусть BN означает двоичный код временного интервала n (от 0 до 7) из 64 бит. Бит I ключа Kcn - Kcn(i) вычисляется как Kcn(i)xor(BN<<32(i)) (где xor – побитовое суммирование, <<32 32-битный циклический сдвиг) количество сложений будет таким что lsb клоча Kc складывается операцией xor с lsb смещенного BN.

Расшифрование производится аналогичным способом.

Для шифрования алгоритм A5 производит, каждые 4.615 ms, последовательность из 114 зашифровающих/расшифровающих бит ключа (далее блок) побитно суммируемых с битами

открытого текста. Первый бит ключа шифрования, произведенный алгоритмом A5, добавляется в e0, второй – в e1 и так далее.

Для каждого канала расшифрование выполняется на стороне MS, BLOCK1 содержит 114 бит ключа шифрования и используется для шифрования и расшифрования блока BLOCK2 поэтому, A5 должен производить два блока каждые 4.615 ms.

Синхронизация обеспечивается введением в A5 переменной времени COUNT получаемой из номера кадра TDMA. Таким образом, каждый 114-битный блок, производимый A5 зависит только от номера кадра TDMA и ключа шифрования Kc.

COUNT состоит и 22 бит соединенных путем конкатенации параметров T1, T3 и T3. Это входные параметры алгоритма A5. Состав переменной COUNT указан на рисунке ниже.

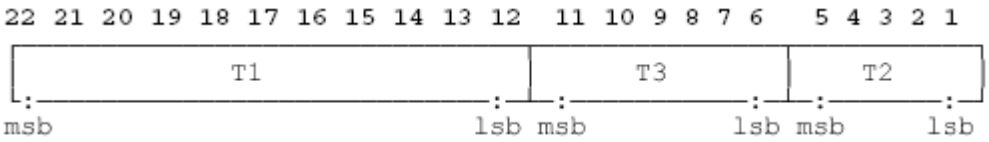

Рисунок 8 Переменная COUNT

Двоичное представление графа. Бит 22 является наиболее значащим битом (MSB) и бит 1 - младший бит (LSB) графа. Значения T1, T3 и T2 представлены в двоичной системе. (Для определения T1, T3 и T2, см. GSM 05,02).

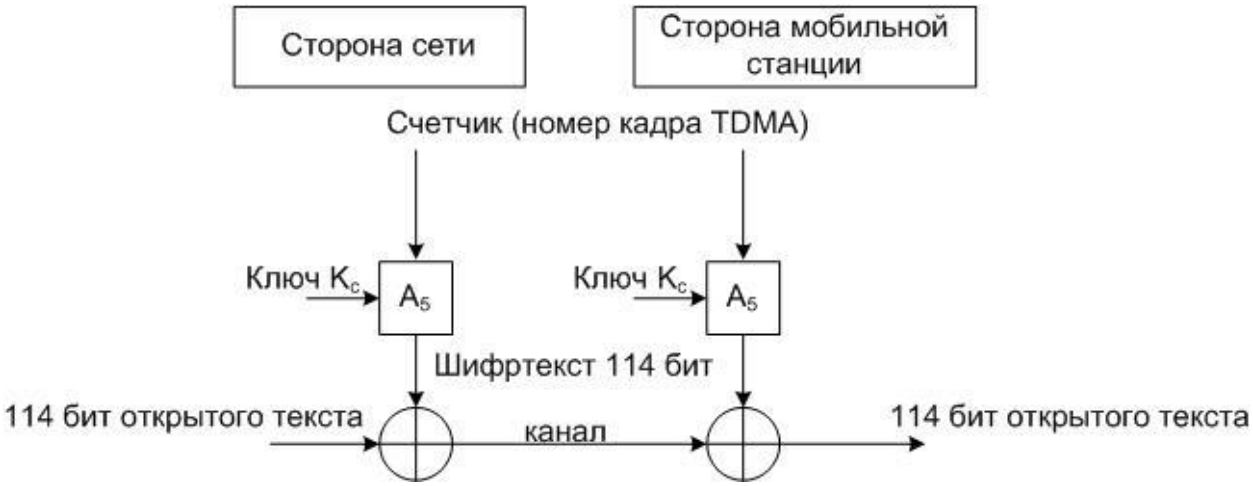

Рисунок 9 Расшифрование на стороне MS

Алгоритм A5 имеет два входных параметра (COUNT и Kc) и выходные параметры (BLOCK1и BLOCK2), которые используют следующие форматы:

Длина ключа Kc – 64 бита;

Длина COUNT – 22 бита;

Длина BLOCK1 – 114 битов;

Длина BLOCK2 – 114 битов.

Алгоритм A5 должен создавать блоки BLOCK1 и BLOCK2 быстрее чем создается один кадр TDMA, то есть за 4.615 ms.

Примечание: Если фактическая длина ключа меньше 64 битов, то шифрование выполняется наиболее значимыми битами ключа Kc, остальные устанавливаются в значение «0».

Алгоритм A3

Алгоритм A3 должен вычислить время ожидания ответа SRES, от генератора случайных чисел RAND присылаемого по сети. Для этих вычислений алгоритм A3 использует секретный ключ аутентификации Ki. На стороне MS, алгоритм A3 содержится в модуле идентификации пользователей (Subscriber Identity Module).

На стороне сети — это реализовано в HLR или в AuC. Два входных параметра (RAND и Ki) и выходной параметр (SRES) алгоритма A3 должны иметь следующий формат:

Длина Ki – 128 бит;

Длина RAND – 128 бит;

Длина SRES – 32 бита.

Время работы алгоритма A3 должно быть больше чем 500 ms.

Алгоритм A8

Использование алгоритма A8 зависит от решения оператора GSM и производится по запросу в GSM/MoU.

На стороне MS, алгоритм A8 содержится в SIM- карте.

На стороне сети A8 располагается совместно с A3.

Два входных параметра (RAND и Ki) и выходной параметр (Kc) алгоритма A8 должны иметь следующие форматы:

Длина Ki – 128 бит;

Длина RAND – 128 бит;

Длина Kc – 64 бита.

Так как максимальная длина ключа шифрования зафиксирована GSM/MoU, A8 должен произвести ключ необходимой длины и расширить его, при необходимости, в 64 битное слово, в котором, наименее значимые биты, равны нулю.

Шифрование в iDEN

Процедура установления защищенного соединения в протоколе iDEN аналогична предыдущему протоколу.

Аутентификация

Название технологии	Аутентификация устройств	Аутентификация процессов	Аутентификация пакетов	Аутентификация пользователей
Bluetooth	По PIN	нет	Нет	нет
UWB	По MAC и SSID	нет	Нет	нет
ZigBee	По MAC и SSID	нет	MIC-64	нет
Insteon	XOR	нет	Есть	нет
Z-Wave				
ANT	Pairing Request,Passkey,Pass-through			
RuBee	По ключу AES			
RFID	Crypto1	нет	Нет	нет
X10	XOR	нет	Есть	нет
WI-FI	WPA 2	нет	TKIP	TKIP
PDC	A3	нет	A3	PIN
IDEN	Ki	нет	Ki	PIN
CDMAOne	CAVE	есть	Есть	PIN
WIMAX	AES	EAP-TLS, PEAP	AES	Parol
GSM	A3	-		PIN
GPRS	A3/A8	-	A3/A8	PIN
UMTS	IMSI	AKA	MAC-I(F9)	USIM

Аутентификация в Bluetooth

Аутентификация в протоколе Bluetooth построена по схеме запрос-отзыв (стратегия идентификации пользователя путём проверки правильности его реакции на непредсказуемый запрос системы). Эта схема предполагает, что запрашиваемое устройство знает секретный сеансовый ключ. В протоколе Bluetooth используется алгоритм аутентификации E1, построенный

по данной схеме. Алгоритм E1 приведен на рис. 6.

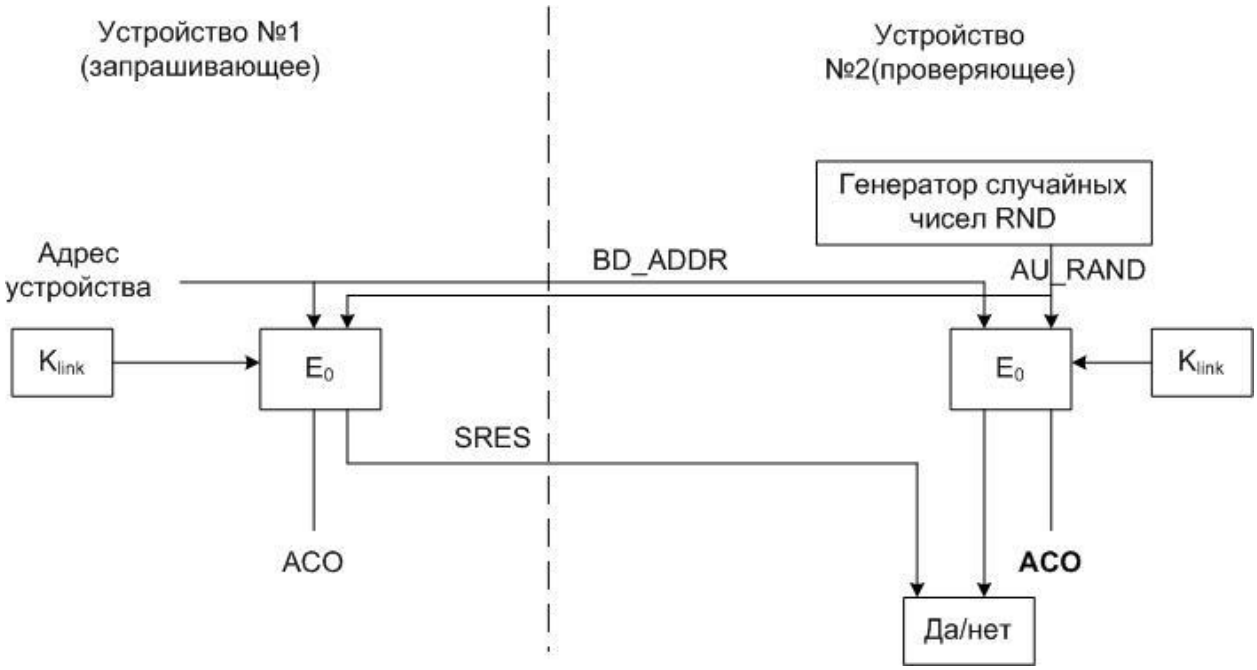

Рисунок 10 Алгоритм аутентификации E1

Схема аутентификации с использованием алгоритма E1(SAFER+):

Проверяемая сторона передает проверяющей 128-битное случайное число AU_RAND;

Проверяющая сторона вычисляет ответ для проверяемой используя алгоритм E1, свой уникальный 48-битный адрес устройства BD_ADDR, сеансовый ключ и выход генератора случайных чисел AU_RAND. Для аутентификации будут использоваться только 32 старших разряда, получаемых после шифрования E1, оставшиеся 96 бит от 128 битного выхода шифра носят название Authenticated Ciphering Offset (ACO) и используются позже для генерации ключа шифрования Bluetooth;

Проверяемая сторона возвращает 32 старших бита как вычисленный ответ SRES;

Проверяющая сторона самостоятельно вычисляет значение SRES и сравнивает его с полученным значением;

Если полученные 32 бита сходятся с вычисленными, то аутентификация проходит, если не сходится – аутентификации не происходит;

Аутентификация в ANT

Отсутствует.

Аутентификация в PDC

Подсистема аутентификации в протоколе PDC состоит из следующей процедуры обмена информацией между сетью и абонентом (MS):

Сеть связи высылает абоненту MS случайное число RAND;

Абонент MS вычисляет подпись для RAND, которая получает название SRES, используя алгоритм A3 и некоторый секрет; (индивидуальный ключ аутентификации абонента – Ki).

Абонент посылает в сеть подпись SRES;

Сеть проверяет SRES.

Вся процедура отображена на рисунке ниже.

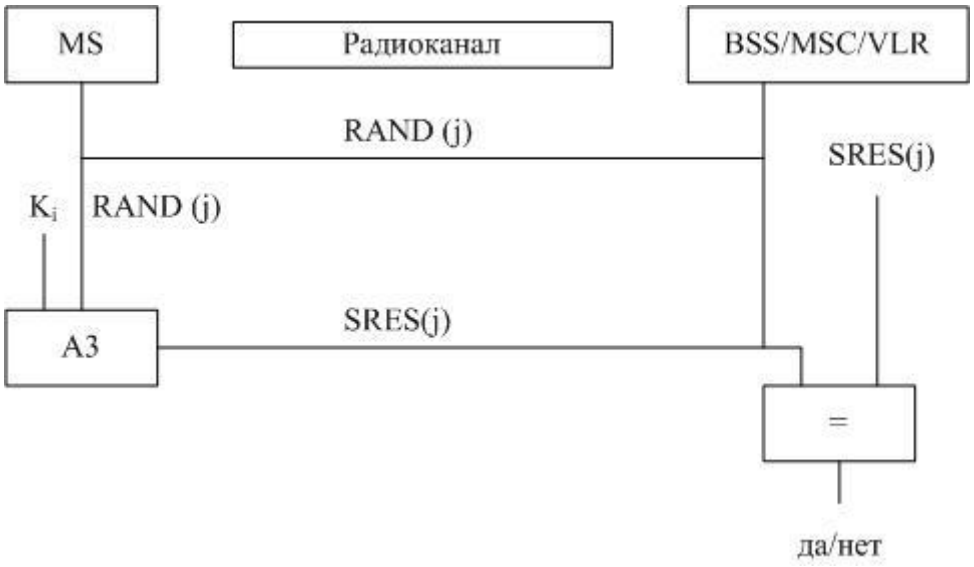

Рисунок 11 Процедура аутентификации

Аутентификация в IDEN

Аутентификация – процедура, использующая алгоритмы создания цифровой подписи с использованием случайного числа. FNE посылает случайное число абоненту, абонент вычисляет подпись данного числа и возвращает ее для сравнения и подтверждения подлинности абонента путем знания ключа шифрования.

Процесс аутентификации — это процесс между абонентом MS и системой iDEN, он позволяет аутентифицировать абонента MS и назначить ему права доступа к сервисам. Абонент аутентифицируется путем использования цифровой подписи.

Во время первоначальной регистрации абонента в сети ему в соответствии ставится IMEI и алгоритм аутентификации (K_i). Базовая станция (HLR) использует алгоритм подписи абонента (MS) для генерации 32 подписей из 32 случайных чисел. После генерации эти числа заносятся в таблицу VLR.

Для аутентификации абонент посылает свой ID в VLR. ID состоит из:

Международный мобильный идентификатор оборудования (IMEI) – при первичной регистрации;

Международный мобильный идентификатор абонента (IMSI) - в процессе регистрации;

Временный мобильный идентификатор абонента (TMSI) – при звонках в роуминге;

IP адрес – для передачи данных по сети.

VLR посылает одно из случайных чисел абоненту. Абонент запускает генератор подписи и вычисляет подпись. Абонент пересылает подпись в VLR. Где она сравнивается со значениями таблицы. По результатам сравнения назначаются права доступа или происходит отказ в них.

Когда абонент MS включает телефон первый раз он походит регистрацию в системе. В процессе регистрации абонент:

Посылает свой IMEI в сеть iDEN FNE.

Получает IMSI изданный DAP/MSC;

Получает остальные параметры сети.

Эти параметры позволяют получить доступ к основному каналу управления сети.

После получения абонентом ID системы, IMEI больше не используется в качестве идентификатора доступа, до тех пор, пока не будут удалены все параметры сети в мобильном телефоне.

Канал радиосвязи содержит специальную информацию согласно протоколам RLP и Mobis.

Информация об абоненте MS включает в себя:

Международный мобильный идентификатор абонента(IMSI);

Аутентификатор Ki;

Временный мобильный идентификатор абонента (TMSI).

IMSI является уникальным идентификатором, который выдает, «домашняя сеть», абоненту MS при инициализации;

Ключ аутентификации (Ki) используется для идентификации MS путем подписывания случайных чисел цифровой подписью.

Случайное число — это часть таблицы, которая используется для аутентификации MS.

Цифровые подписи — это часть таблицы, которая используется для аутентификации MS.

TMSI – это временный идентификатор абонента в роуминговых сетях, который используется для аутентификации MS, пока он активен в данной сети. Этот параметр ограничивает рассылку различных пакетов сильнее, чем при использовании идентификатора IMSI. IMSI присваивается абоненту, как только он появляется в «домашней сети».

Пароли

Название технологии	Установка пароля	Смена пароля	Черные/белые листы	Контроль качества
Bluetooth	Да	Да	Нет	Нет
UWB	Да	Да		
ZigBee	Да	Да		
Insteon	Да	Да		
Z-Wave	Да	Да		
ANT	Нет	Нет		
RuBee	Да	Да		
RFID	Нет	Нет		
X10	Нет	Нет		
WI-FI	Да	Да		
PDC	Да			

IDEN	Да	Да		
CDMAOne	Да	Да		
WIMAX	Да	Да		
GSM	Да	Да		
GPRS	да	Да		
UMTS	да	Да		

Управление ключами в PDC

Ключ назначается абоненту при первом включении абонента в домашней сети. Ключ меняется с каждым сеансом путем шифрования случайного числа RAND/ SRES ключом K_i при помощи алгоритма A3.Процедура смены ключа сеанса представлена на рисунке ниже.

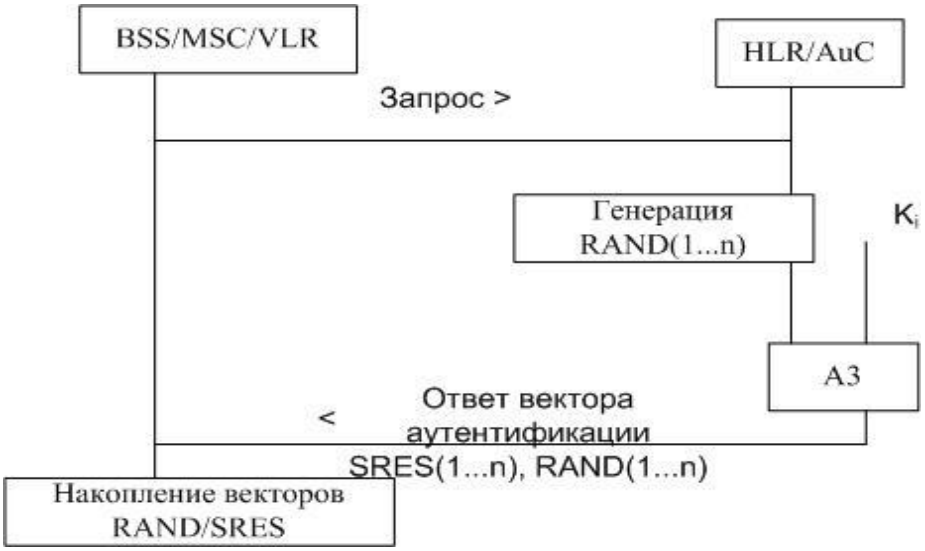

Рисунок 12 Процедура смены ключа сеанса связи в протоколе PDC

В данной схеме BSS/MSC/VLR - это стационарные станции сети связи, которые управляют сетью. HLR/AuC – подвижные станции сети PDC, на которых выполняется генерация случайных чисел RAND, хранение ключа K_i и генерация векторов аутентификации SRES.

Алгоритм управления ключами - A8 (GSM/GPRS)

Использование алгоритма A8 зависит от решения оператора GSM и производится по запросу в GSM/MoU.

На стороне MS, алгоритм A8 содержится в SIM- карте.

На стороне сети A8 располагается совместно с A3.

Два входных параметра (RAND и K_i) и выходной параметр (K_c) алгоритма A8 должны иметь следующие форматы:

Длина K_i – 128 бит;

Длина RAND – 128 бит;

Длина K_c – 64 бита.

Так как максимальная длина ключа шифрования зафиксирована GSM/MoU, A8 должен произвести ключ необходимой длины и расширить его, при необходимости, в 64 битное слово, в котором, наименее значимые биты, равны нулю.

Уязвимости и риски

Уязвимости

Ниже представлены основные уязвимости для беспроводных протоколов

№	Уязвимость	Пояснения
1	Ключ устройства используются повторно и скомпрометированы	Ключ устройства должен быть использован для генерации случайного ключа. Должен использоваться набор ключей, а не один ключ.
2	Ключи при обмене перехватываются	Коррумпированных пользователь может поставить под угрозу безопасность двух других пользователей, если коррумпированный пользователь общался с любой из двух других пользователей.
3	Слабое управление PIN-кодами	Слабые PIN-коды, которые используются для генерации ссылки и ключи шифрования, легко угадать. Люди имеют тенденцию выбирать короткий PIN-кода.
4	Ключ для шифрования повторяется после 23.3 часов его применения (в BlueTooth)	В шифре E0, ключ шифрования потока зависит от ключа соединения, EN_RAND, Master BD_ADDR, и времени. Только время будет меняться в течение определенного защищенного соединения. Если связь длится больше чем 23,3 часов, значение времени начнет повторяться, следовательно, порожденная гамма идентична использованной ранее в связи.
5	Ненадежное хранения ключей	Ключи сеанса могут быть прочитаны или изменены злоумышленником, если они не надежно сохраняются и защищаются с помощью контроля доступа.
6	Повтор попыток аутентификации	Функция ограничения количества попыток аутентификации должна быть включена. В стандарт включено требования по экспоненциальному росту времени
7	Стойкость запрос-ответа генератора псевдослучайных чисел не известна	ГСЧ может произвести последовательность чисел со статической зависимостью, что ослабит схему аутентификации.
8	Ключ изменяемой длины	Минимально допустимый размер ключа – 1 байт, что является недостаточным для обеспечения безопасности.

9	Главный ключ открытый	Улучшенная схема распределения ключей должна быть включена в протокол.
10	Нет аутентификации пользователей	Согласно спецификации, производится только аутентификация устройств
11	Используется слабый алгоритм шифрования E0	Необходим более защищенный алгоритм шифрования
12	Конфиденциальность может быть нарушена, если адрес Bluetooth устройства (BD_ADDR) захватывается и связан с конкретным пользователем	
13	Аутентификация устройства построена на очень простом и слабозащищенном принципе раскрытия секрета «запрос-ответ»	Такой тип аутентификации уязвим для MITM атаки
14	Защита канала точка-точка не выполняется	При использовании ретрансляторов данные на них расшифровываются
15	Обеспечение безопасности очень ограничено	Аудит и контроль целостности стандартом не предусмотрен, но эти функции могут быть реализованы внешним ПО.
16	В процессе обнаружения и подключения устройства уязвимы для атак	Режим поиска подключения должен отключатся, когда в нем нет необходимости.

Риски

Риск прослушивания

Самый существенный риск, заключается в пассивном прослушивании канала третьей стороной. Существует несколько методов организации прослушивания:

1. Подслушивание абонента при громком разговоре;
2. Прослушивание при помощи закладок в помещении;
3. Перехват беспроводного соединения;
4. Перехват информации на узлах сети;
5. Перехват информации при передаче между узлами сети;

Риск кражи записей информации

Данный риск характерен для автоответчиков и телефонов с функцией диктофона. Суть данного риска заключается в возможности воровства записанной информации с носителей. В

роли носителей выступают автоответчики телефонов, память диктофонов, совмещенных с телефонами, память узлов сенсорных сетей и т.д.

Анализ передаваемого потока управления

Для злоумышленника может представлять интерес любая информация о действиях пользователя:

- Время и дата разговоров и сеансов передачи данных;
- Вызываемые абоненты;
- Местоположение абонентов;
- Номера и IP адреса абонентов;
- История сеансов связи;
- Телефонная книга и перечень адресов.
- Определение местоположения.

Этот риск характерен для любого пользователя передающего устройства, находящегося в сети с промежуточными устройствами. Например, для пользователей сотовых телефонов.

Прочие риски

Загрузка кода

Существующие беспроводные устройства слабо защищены от загрузки программного кода и его исполнения на узлах сети. Этот код может работать в интересах третьей стороны и наносить ущерб системе передачи информации, передаваемой информации и пользователям системы.

Восстановление удаленных сообщений

Особенности электронной памяти, используемой в современных беспроводных устройствах таковы, что она может долго сохранять в себе ранее удаленную информацию. Это связано так же с алгоритмами удаления – как правило, разработчики программного обеспечения ограничиваются стиранием ссылок на записанную информацию или заголовков, не затирая саму информацию.

Кражи

Одним из самых существенных рисков для узлов беспроводных сетей является риск кражи самих узлов. Это связано как с ценностью самих узлов, так и с отсутствием возможности контролировать распространение и перепродажу краденых узлов беспроводных сетей.

Атаки на беспроводные сети

Для беспроводных сетей характерны следующие виды атак:

1. Отказ в обслуживании (DoS);
2. Пассивное прослушивание (eavesdropping);
3. Атака «человек-по-середине» (man-in-the-middle attacks);
4. Модификация сообщений (message modification);

5. Захват ресурса(resource misappropriation).

Модель угроз

Для всех представленных беспроводных технологий характерны угрозы нарушения целостности, конфиденциальности и доступности информации.

При этом, вне зависимости от топологии и протокола связи пути реализации этих угроз будут следующие:

1. Перехват ключа шифрования при обмене между устройствами;
2. Использование старых (неизменяемых или скомпрометированных) ключей шифрования;
3. Ненадежное хранение ключей шифрования – в случае вирусной атаки или несанкционированного доступа к узлу сети можно получить ключ шифрования;
4. В ряде технологий отсутствуют или сильно урезаны процедуры аутентификации устройств, процессов, пакетов и пользователей;
5. Используются небезопасные протоколы установления соединений;
6. Стойкости используемых алгоритмов шифрования, как правило, недостаточно.

При этом следует учитывать, что в роли криптоаналитика может выступать как узел, не находящийся в сети, так и узел, являющийся ее частью.

Модель криптоаналитика

Для сенсорных сетей всех типов характерна модель криптоаналитика, представленная в [31][32]. Возможности криптоаналитика заключатся в:

1. Перехват сообщений и их взлом;
2. Модификации блоков данных, как в канале, так и на узлах сети;
3. Подделки авторства передаваемых блоков;
4. Повторной передаче устаревших блоков данных;
5. Отказе передавать далее принятые блоки данных.

В первом случае, криптоаналитик представлен «надежным, но любопытным узлом» он принимает и передает все принятые пакеты. Но при этом, копирует их и пытается взломать. Вероятность взлома в данном случае сильно зависит от местоположения узла в сети. Чем ближе он находится к источникам данных, до осуществления сетевого кодирования другими узлами, тем проще криптоаналитику получить исходное сообщение или его часть.

---

[31] Lima L., Vilela J., Oliveira P., Barros J., Filiz I., Guo X., Morton J., Sturmfels B., Mungan M., Ramasco J. [et al.] Network Coding Security Attacks and Countermeasures. 2008.

32 Buttyŕan Levente, ŕo Czap Lŕaszl, Vajda Istvŕan. Pollution Attack Defense for Coding Based Sensor Storage Proceedings of the Conference of the IEEE Computer and Communications Societies (INFOCOM), Anchorage, Alaska, USA, 2010.

Модели прослушивающего криптоаналитика, приводимые в современной литературе сводятся, как правило, к задаче восстановления исходного текста из перехватываемых сообщений из одного или нескольких (подмножества) каналов. В работах[33] [34] [35] представлено обоснование условий использования теоретически-стойких систем шифрования в системах с линейным кодированием и несколькими источниками информации.

Так же применима схема криптоаналитика, когда предусмотрено знание им всех передаваемых открытых текстов. В данном случае, для защиты системы передачи данных используется линейное кодирование с подбором коэффициентов сети[36].

Заключение

Беспроводные сети получили широкое распространение в повседневной жизни и динамика процесса распространения такова, что количество беспроводных сетей будет только увеличиваться. Ценность информации, передаваемой по беспроводным сетям растет вместе с количеством информации и сетей.

Используемые криптографические алгоритмы и протоколы не обеспечивают необходимого уровня защиты передаваемой, хранимой и обрабатываемой информации. Причинами этого является: недостаточная криптографическая стойкость алгоритмов шифрования к атакам, в том числе атаке «грубой силы»; отсутствие надежных протоколов смены и генерации ключей; отсутствие или слабые протоколы аутентификации узлов и передаваемых информационных пакетов.

Анализ защищенности беспроводных протоколов и устройств в Wi-Fi пространстве в настоящее время оценивается в рамках модулей оценки уязвимостей в сканерах уязвимостей. Учитывая, что критически важная инфраструктура предприятия должна оцениваться по протоколу SCADA и включать все уровни информационной среды начиная от канального и заканчивая уровнем приложений то необходимо использование сканеров уязвимостей промышленного уровнять. На данный момент в России представлены отечественные – MaxPatrol и зарубежные системы оценки защищенности предприятия, например - система Tenable Security Center используемая в Европе и США с 2000 года и развивающаяся частично в России командой разработчиков с поддержкой стандартов NICT, FISMA.

---

[33] Cai N., Yeung R. Secure network coding // Proceedings of the IEEE International Symposium on Information Theory. Lausanne, Switzerland. 2002.

[34] Cai N., Yeung R. Network error correction // Proceedings of the IEEE International Symposium on Information Theory, Yokohama, Japan, July. 2003.

35 Cai N., Yeung R. W. A Security Condition for Multi-Source Linear Network Coding //IEEE International Symposium on Information Theory (ISIT). Nice, France. 2007.

36 Lima L., Vilela J. P., Barros J., Medard M. 2008. An Information-Theoretic Cryptanalysis of Network Coding — is protecting the code enough? // International Symposium on Information Theory and its Applications, ISITA2008. Auckland, New Zealand.

Из всех рассмотренных протоколов только протоколы Z-wave, UWB. ZigBee, Wi-Fi, Wimax обладают шифрами устойчивыми ко взлому в достаточной мере, что бы противостоять атакам грубой силы – 3DES, AES. Все остальные протоколы располагают алгоритмами шифрования со стойкостью к взлому не более чем 2^{38}, что приблизительно равно $10^{11,44}$. Такого уровня стойкости абсолютно недостаточно, так как для вычислительной системы на базе процессора Core 2Quad Q6600 выполняющем до 17,6 миллиардов операций в секунду, то есть около 10^{10} вычислений. Для перебора всех ключей таких алгоритмов понадобится не более 20-15 минут. Для перебора ключей DES с длиной ключей 56 бит понадобится около 42 дней.

- Для современных беспроводных систем связи необходим шифр со стойкостью к взлому не менее 2^{92} вариантов ключей;
- Необходима надежная схема смены симметричных ключей;
- Необходима возможность вести широковещательную рассылку на симметричных алгоритмах.
- Алгоритм шифрования должен максимально использовать свойства сети, топологий, устройств для обеспечения безопасности.

При этом несомненным плюсом рассмотренных протоколов следует считать возможность создания и использования криптографических протоколов на верхних уровнях протоколов передачи данных.

Защита ключевых систем информационной инфраструктуры

Подход к защите ключевых систем информационной инфраструктуры ничем не отличается от классических подходов обеспечения информационной безопасности в ИТ – инфраструктуре. За исключением, того, что порядок внедрения и требования к подсистемам безопасности могут регулироваться разными нормативными документами в зависимости от того, в какой отрасли применяется система защиты информации. Именно поэтому далее приведен лишь этап аудита этих систем. Этапы внедрения, эксплуатации и переоценки не рассматриваются.

Аудит

Для того, чтобы понимать, что и от чего мы защищаем, необходимо предварительно составить перечень используемых в критичных системах информационной инфраструктуры различных программных и программно-аппаратных компонентов. Причем, эта процедура должна выполняться на постоянной периодической основе при помощи технических средств. Такой класс систем называется системами управления активами (по-английски asset management).

Системы управления активами достаточно развиты для технических компонентов ИТ систем, но их использование в сетях ключевых систем информационной инфраструктуры будет

ограничено подсистемами, которые используют для передачи данных протокол TCP/IP, все остальные системы, будь то заводской насос аммиака под управлением АСУ ТП и работающий по протоколу MODBUS или система управления воздушным движением ADS-B работающая в ближайшем аэропорту в это исследование не попадут.

В то же время, если рассмотреть пример с системой контроля воздушного движения (КПВ) то следует признать эту систему критичной, так как она может одновременно выдавать управляющие сигналы и проводить контроль обширной зоны воздушного движения с большим количеством самолетов и пассажиров на них. В тоже время, эта система будет являться предельно уязвимой для атак хакеров, так как в ней нет встроенных систем шифрования каналов между компонентами системы, а это означает, что любой, подключившийся к такому каналу способен внести изменения в передаваемую информацию и ее перехватить.

Ключевые системы информационной инфраструктуры часто обязаны работать постоянно в режиме реального времени. Выход из строя подобной системы и неработоспособность дублирующего оборудования может привести к блокировке трафика отдельного аэропорта, что и произошло в августе 2013 года в аэропорту им. Ататюрка г. Стамбула, Турция. В результате эффективной атаки хакеров на систему паспортного контроля была заблокирована работа аэропорта на два часа. Что привело к переносу рейсов и значительным тратам авиакомпаний на топливо и простой самолетов в аэропорту. (http://thehackernews.com/2013/07/Istanbul-airport-cyber-attack-virus.html). Сами ключевые системы информационной инфраструктуры являются уязвимыми, к примеру, в ADS-B отсутствует шифрование трафика, аутентификация пользователей, что позволяет хакеру искажать информационный обмен между центром управления полетами и летчиком.

На этапе обследования следует обеспечить решение следующих задач:

- выявление уязвимостей оборудования ключевых систем информационной инфраструктуры и программной платформы ключевых систем информационной инфраструктуры;
- выявление возможности получения несанкционированного доступа к системе КВП или отдельным ее компонентам;
- базовая оценка отказоустойчивости ключевых систем информационной инфраструктуры;
- выявление недостатков в применяемых Заказчиком мерах информационной безопасности и оценка возможности их использования нарушителем;

- аудит и проверка конфигурации на соответствие стандартам безопасности и лучшим практикам лидеров индустрии;
- получение на основе объективных свидетельств экспертной оценки текущего уровня защищенности ключевых систем информационной инфраструктуры;
- разработка рекомендаций по устранению выявленных уязвимостей и повышению уровня защищенности ключевых систем информационной инфраструктуры.

Работы по комплексному анализу защищенности проводятся в три этапа разными группами специалистов Исполнителя и включают в себя:

- Первый этап Группа 1:
  - анализ защищенности сетевого периметра локальной вычислительной сети (тестирование на проникновение) Заказчика от атак со стороны злоумышленника, действующего в сети Интернет;
  - анализ защищенности ключевых систем информационной инфраструктуры от атак со стороны сети Интернет методом «черного-ящика». На данном этапе используется модель внешнего злоумышленника, не обладающего никакими сведениями и логическим доступом к Системе;
  - оценка эффективности программы повышения осведомленности в отношении персонала, поддерживающего разработку и эксплуатацию Системы по методике, предварительно согласованной с Заказчиком.
- Первый этап Группа 2:
  - анализ защищенности ключевых систем информационной инфраструктуры от атак со стороны сети Интернет от лица злоумышленника, обладающего пользовательским доступом к системе АСБ;
  - анализ исходного кода веб-приложения Системы методом «белого ящика»;
  - анализ защищенности веб-приложения и аудит типовой конфигурации терминала самообслуживания.
- Второй этап Группа 1:
  - инструментальный аудит и анализ конфигурации всех компонентов Системы (сетевое оборудование, ОС, БД и т.д.) на соответствие стандартам безопасности и лучшим практикам лидеров индустрии.
- Второй этап Группа 2:

- анализ защищенности (тестирование на проникновение) технологического сегмента ЛВС, в котором расположено оборудование, поддерживающее Систему Заказчика, от атак со стороны внутреннего злоумышленника.

- Второй этап Группа 3
  - анализ защищенности ключевых систем информационной инфраструктуры от лица злоумышленника, обладающего административным доступом к ключевой системе информационной инфраструктуры.
- Третий Этап
  - проведение нагрузочного тестирования ключевых систем информационной инфраструктуры с целью оценки устойчивости к распределённым атакам типа «отказ в обслуживании» (DDOS).
- Четвертый Этап
  - Анализ данных собранных в результате авторизации пользователей и взаимодействия компонентов информационной структуры на предмет оценки соответствия стандарту по информационной безопасности для архитектуры SCADA или стандарта PCI DSS на уровне используемых приложений и правильности установки средств защиты информации.

Целью каждого этапа является выявление максимально широкого круга уязвимостей, анализа риска использования той или иной системы, в ходе эксплуатации которых возможно реализовать атаку на ключевые компоненты Системы, и оценка потенциальных негативных последствий подобных атак. Применяемые в современных SIEM системах методики анализа состояния ИБ обеспечивают выявление существующих недочетов, допущенных в ходе проектирования, разработки и эксплуатации ИС, практическую демонстрацию возможности использования уязвимостей (на примере наиболее критических) и формирование рекомендаций по устранению выявленных уязвимостей на основе стандартов безопасности.

Пример атаки на ключевой объект инфраструктуры мегаполиса

В подтверждении важности и актуальности всего вышеизложенного материала в этой главе приведен реальный практический пример взлома реальной системы АСУ ТП жизненно важного инфраструктурного объекта одного из мегаполисов. Взлом проводился в ходе официального обследования сети этого объекта на предмет уязвимости к внешним хакерским

атакам. В результате обследования была доказана его уязвимость. Подобная сеть является типовой и обязательно присутствует в каждом городе. Нарушение работоспособности подобных сетей может привести к огромным финансовым потерям и поставить на грань выживания всех жителей атакованного мегаполиса. Потому, аналогичные системы, следует считать одними из самых приоритетных среди потенциальных объектов кибертерроризма.

Общая архитектура сети

В рассматриваемой сети АСУ ТП представляет собой совокупность программных и аппаратных средств. Комплекс состоит из компьютеров, объединенных в локальную вычислительную сеть (далее - ЛВС) на базе ОС Windows, аппаратуры сбора данных и прикладного программного обеспечения.

Структурная схема АСУ ТП представлена на рисунке ниже.

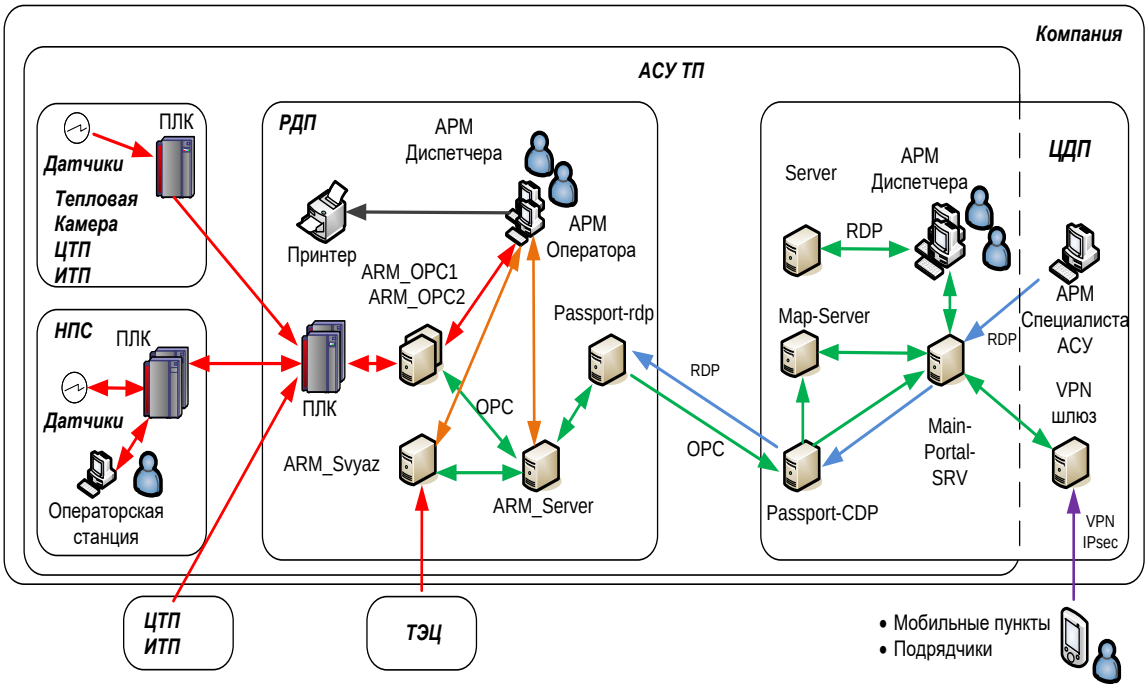

Рисунок 13 Структурная схема АСУ ТП

Типовая схема РДП представлена ниже.

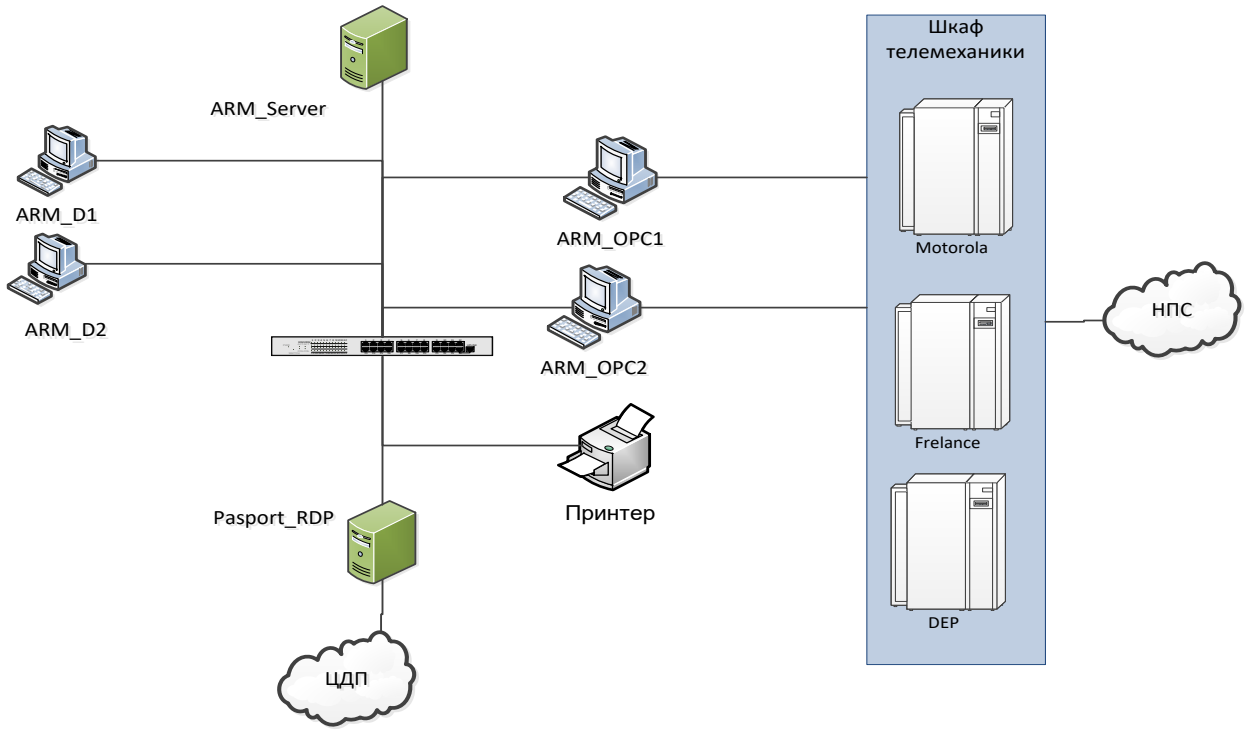

Рисунок 14Типовая схема РДП

Типовая схема НПС представлена ниже.

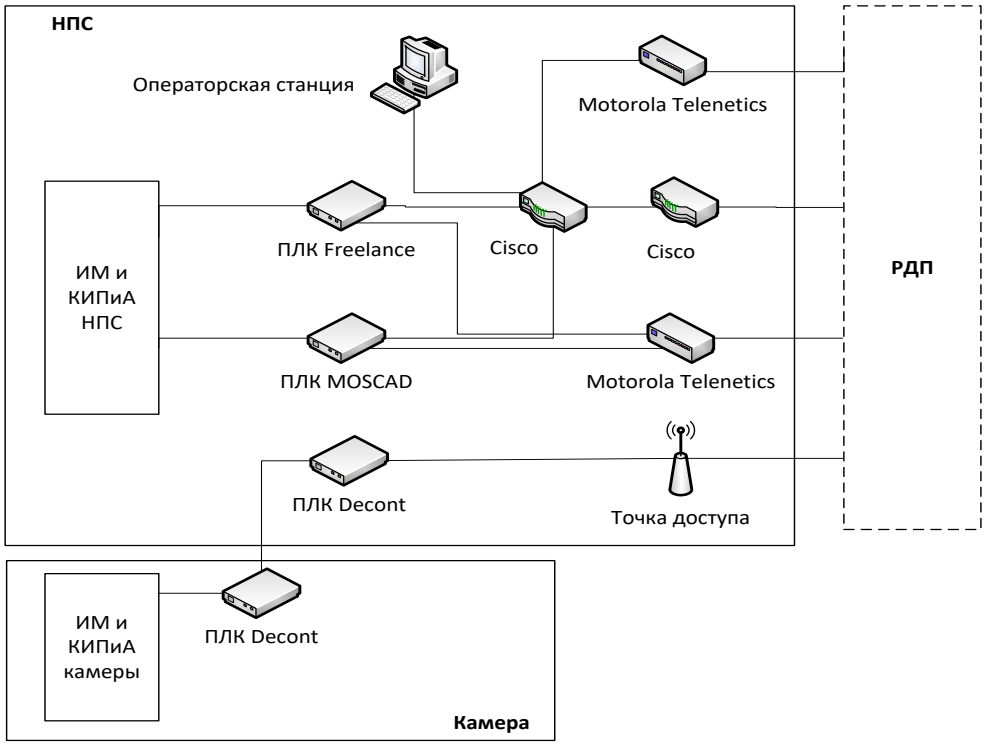

Рисунок 15 Типовая схема НПС

Типовая схема Тепловой камеры представлена ниже.

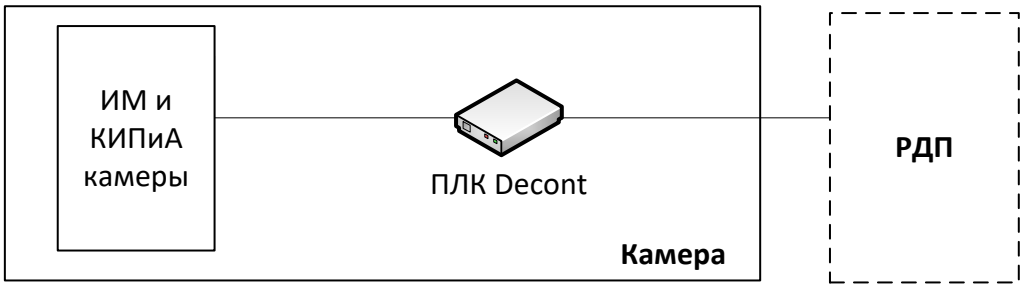

Рисунок 16 - Типовая схема Тепловой камеры

Перечень компонентов АСУ ТП и их назначение.

№ п/п	Компонент	Назначение
1	ARM_OPC	Ввод-вывод данных по протоколу OPC (конвертация из специфичных протоколов конкретных типов контроллеров в стандартный протокол OPC), мониторинг и диагностика текущих значений параметров в программах OPC серверов
2	ARM_Svyaz	Прием телеметрических данных, поступающих с ТЭЦ
3	ARM_Server	Разграничение доступа, администрирование ЛВС, аварийно-предупредительная сигнализация, ведение исторических трендов и архивов
4	Passport-rdp	Управление техническими средствами АСУ ТП данной РДП посредством терминальной сессии с удаленного АРМ специалиста АСУ, передача телеметрических данных в ЦДП
5	ПЛК	Ввод-вывод параметров: температуры, давления, расхода сетевой воды, положения оборудования, аварийной сигнализации
6	АРМ_Диспетчера	Контроль и управление технологическим процессом: — отображение мнемосхем объектов с реальным состоянием оборудования; — отображение паспортов (окон) управления; — выдача управляющих воздействий на технологическое оборудование; — отображение аварийно-предупредительной сигнализации; — отображение, настройка и печать архивов; — автоматическое и ручное заполнение «Режимной карты», ее отображение и печать; — отображение, настройка и печать графиков истории параметров; — отображение, настройка и печать графиков реальных параметров; — автоматическое резервирование данных (переключение на резервный Server_OPC при отказе основного); — синхронизация локального времени по серверу часов единого времени; — диагностика соединений OPC
7	АРМ_Оператора	Контроль технологического процесса: — отображение мнемосхем объектов с реальным состоянием оборудования;

№ п/п	Компонент	Назначение
		— отображение паспортов (окон) управления; — отображение аварийно-предупредительной сигнализации; — отображение, настройка и печать архивов; — автоматическое и ручное заполнение «Режимной карты», ее отображение и печать; — отображение, настройка и печать графиков истории параметров; — отображение, настройка и печать графиков реальных параметров; — автоматическое резервирование данных (переключение на резервный Server_OPC при отказе основного); — синхронизация локального времени по серверу часов единого времени; — диагностика соединений OPC
8	Операторская станция	Контроль и управление технологическим процессом. Программирование и контроль работы ПЛК
9	Принтер	Печать отчетов
10	Датчики	Съем информации с исполнительных механизмов, управление исполнительными механизмами
11	Main-portal-SRV	АСУ ТП предоставляет доступ к порталу и возможность просматривать мнемосхемы объектов теплосети из всех районов и контролировать параметры телемеханики, получает возможность работы с порталом КИКС
12	Map-server	Корпоративная Информационно-Картографическая Система (КИКС). База данных карты теплосетей, справочник, схема повреждений теплосети

Связь между техническими площадками АСУ ТП организована следующим образом:

а) между ЦДП и РДП – через общую корпоративную сеть и VPN на базе сети внешнего провайдера;

б) между РДП и НПС:

1) через коммутаторы общей корпоративной сети Cisco и через каналы L2 VPN на базе сети провайдера;

2) через последовательные интерфейсы маршрутизаторов сети АСУ ТП Cisco с помощью модемных линий;

3) через модемные линии напрямую между контроллерами, установленными на РДП и на НПС;

в) между РДП и другими технологическими площадками – через последовательные интерфейсы серверов АСУ ТП с помощью модемных линий, а также через медиа-конвертеры Ethernet.

АРМ администраторов ресурсов АСУ ТП расположены в общей пользовательской сети на площадке АСУ/СОТИН. Также для администраторов АСУ ТП реализован удаленный доступ к сети с помощью Cisco VPN Client. Сессии удаленного доступа терминируются на отдельном МЭ Cisco ASA, установленном на границе с сетью интернет.

На рисунках ниже представлены схемы сетевой инфраструктуры АСУ ТП.

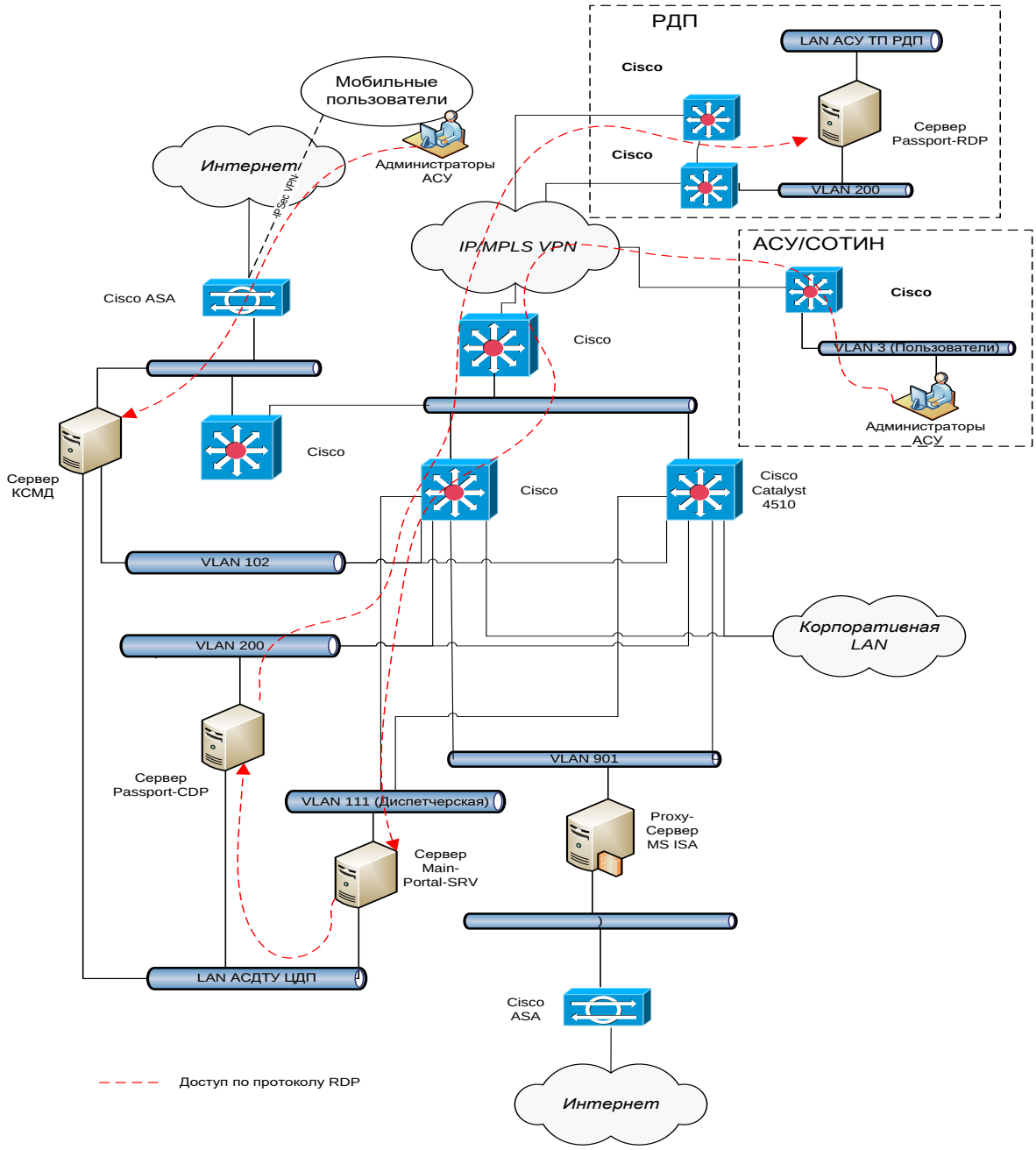

Рисунок 17 - Схема сети ЦДП и ее подключений к удаленным площадкам

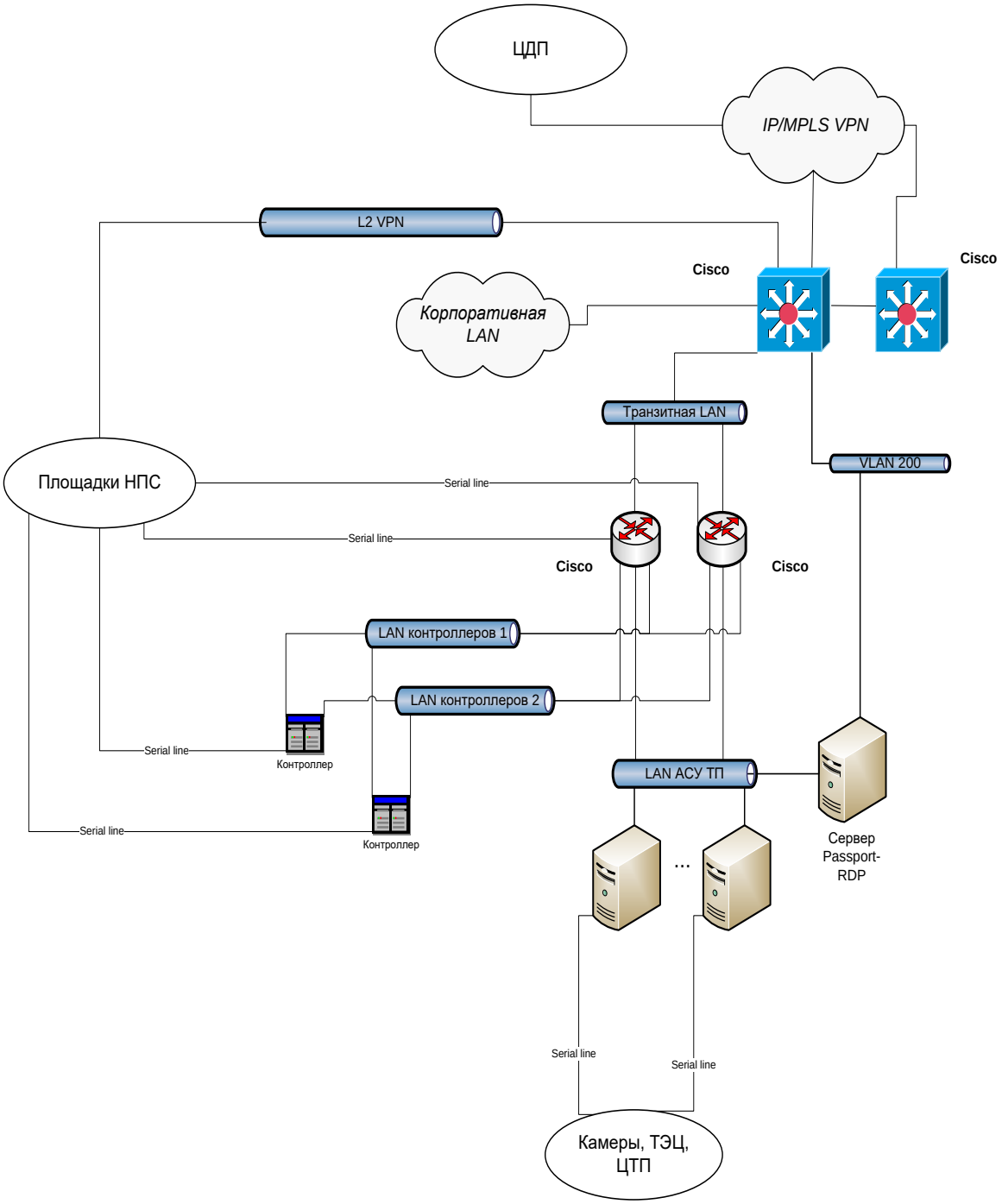

Рисунок 18 - Типовая схема сетевой инфраструктуры РДП

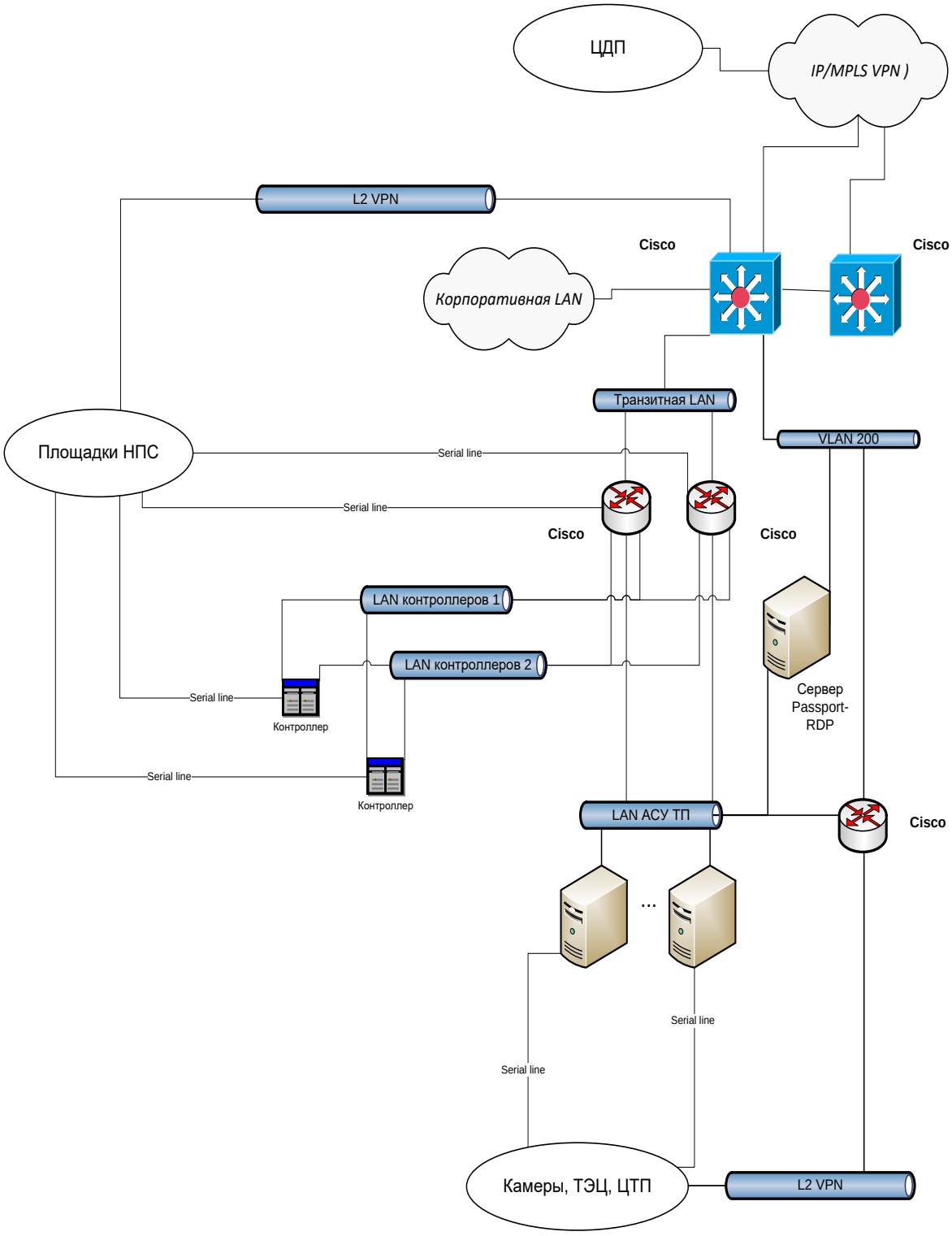

Рисунок 19 - Типовая схема сетевой инфраструктуры РДП

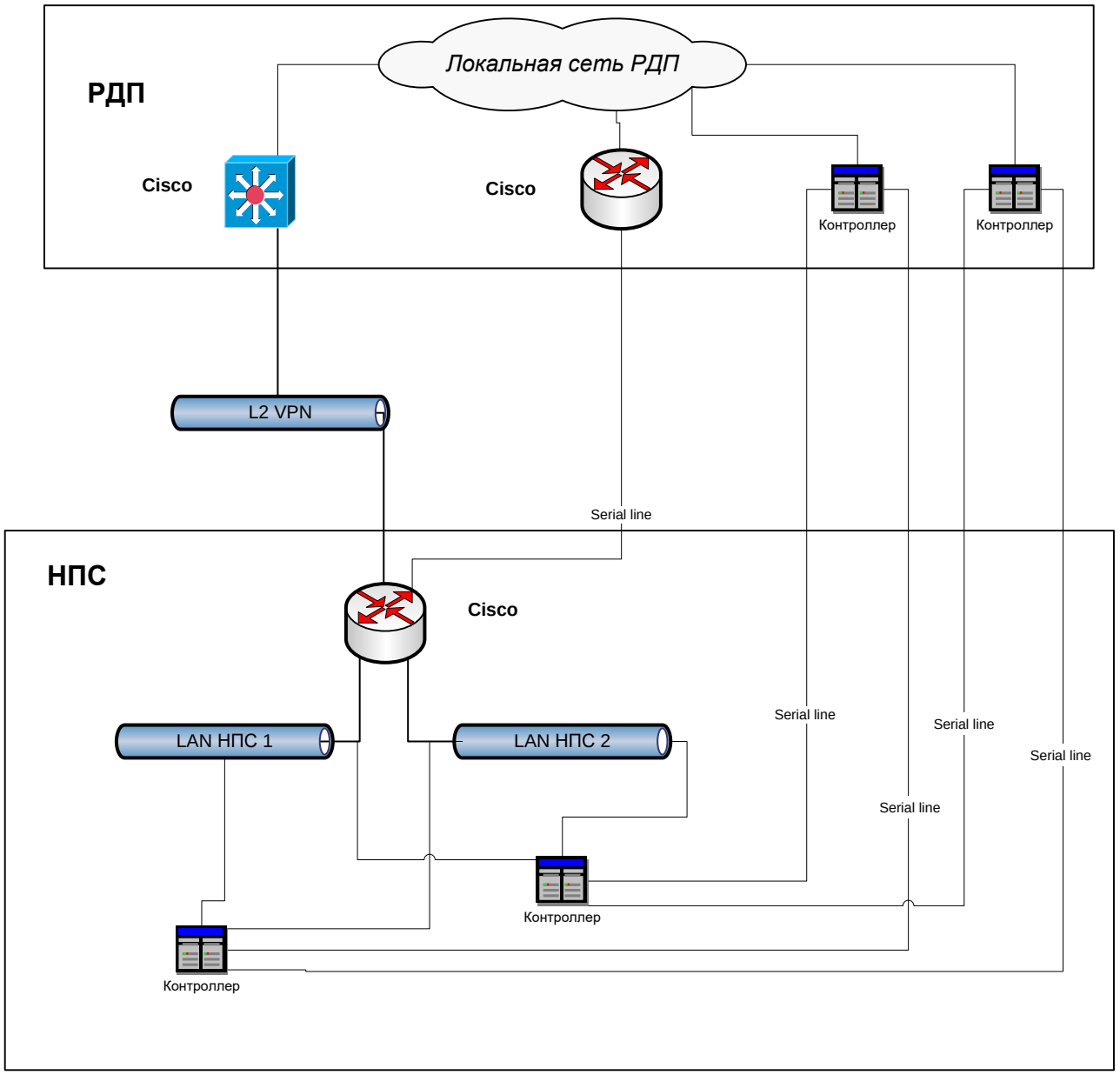

Рисунок 20 - Типовая схема сетевой инфраструктуры НПС и ее подключения к РДП

Сетевая безопасность

В результате обследования рассмотренных сетей были получены результаты, описанные ниже.

Было обнаружены неактуальные правила межсетевого экранирования и правила межсетевого экранирования, обеспечивающие избыточный доступ.

Описание недостатка

На межсетевом экране обнаружен ряд неактуальных правил фильтрации, разрешающих доступ к неактивным сервисам. В частности, существуют правила, разрешающие административный доступ к неактивному на текущий момент оборудованию.

Административный доступ к межсетевому экрану Cisco ASA разрешен по протоколу HTTP для нескольких адресов, не принадлежащих Компании.

Описание выявленного риска

Наличие неактуальных или избыточных правил межсетевого экранирования позволяет внешнему злоумышленнику использовать эти правила для обхода защиты на сетевом уровне.

Степень риска – средняя.

Не была настроена фильтрация сетевого трафика между внутренними сегментами сети.

Описание недостатка

Между внутренними сегментами сети отсутствует фильтрация сетевого трафика.

Трафик из внутренней сети к почтовому серверу и прокси-серверу не фильтруется.

Описание выявленного риска

Отсутствие фильтрации между сегментами сети позволяет внутреннему злоумышленнику получать доступ к любым сетевым сервисам, предоставляемым информационными системами.

Степень риска – высокая.

Было обнаружено что, на межсетевом экране не обеспечивается защита от подмены IP-адресов.

Описание недостатка

Настройками межсетевого экрана Cisco ASA не обеспечивается защита от атак типа спуфинг[37].

Описание выявленного риска

Подменив свой IP-адрес на внутренний, злоумышленник имеет возможность обойти правила фильтрации на межсетевом экране.

Степень риска – высокая.

Управление доступом и учетными записями

Обнаружено использование настроек по умолчанию для сервиса «Подключение к удаленному рабочему столу».

Описание недостатка

Для сервиса «Подключение к удаленному рабочему столу» используются настройки, заданные по умолчанию: шифрование управляющего трафика, задается на стороне клиента, сертификаты не используются, список пользователей, которым разрешено подключение, не задан.

Описание выявленного риска

Так как протокол RDP, на основе которого работает служба «Подключение к удаленному рабочему столу» операционной системы Windows, уязвим к атаке человек посередине[38], использование его без сертификатов (то есть двухфакторной аутентификации) несет риск компрометации доменной учетной записи администратора, а, следовательно, и всех ресурсов, к которым для нее есть

---

[37] IP-спуфинг – вид атаки, заключающийся в использовании чужого IP-адреса с целью обмана системы безопасности.

[38] Атака «человек посередине» (англ. Man in the middle, MitM-атака) – термин в криптографии, обозначающий ситуацию, когда атакующий способен читать и видоизменять по своей воле сообщения, которыми обмениваются корреспонденты, причем ни один из последних не может догадаться о его присутствии в канале.
Метод компрометации канала связи, при котором взломщик, подключившись к каналу между контрагентами, осуществляет активное вмешательство в протокол передачи, удаляя, искажая информацию или навязывая ложную.

доступ. Поскольку текущими настройками уровень шифрования управляющего трафика определяется на стороне клиента, существует риск, что на клиенте будет разрешено нешифрованное удаленное подключение, и тем самым пароль администратора может быть скомпрометирован путем прослушивания трафика.

Степень риска – средняя.

Была найдена возможность получения удаленного доступа к межсетевому экрану по небезопасному протоколу Telnet

Описание недостатка

Для администрирования сетевого оборудования преимущественно используется протокол SSH, но также разрешен удаленный доступ по протоколу Telnet.

Описание выявленного риска

Протокол Telnet в настоящее время считается устаревшим и небезопасным, так как не шифрует передаваемый трафик, в том числе и пароли, которые также передаются в незашифрованном виде и, таким образом, могут быть скомпрометированы путем прослушивания трафика.

Степень риска – высокая.

Наличие возможности удаленного доступа к АРМ «Клиент-Банк»

Описание недостатка

На АРМ «Клиент-Банк» запущен сервис «Подключение к удаленному рабочему столу», позволяющий удаленное подключение по протоколу RDP, также удаленный доступ возможен посредством ПО «Radmin».

Описание выявленного риска

Удаленное администрирование критичных ресурсов (например, АРМ с установленными системами «Клиент-Банк») создает дополнительный вектор атаки, так как злоумышленник, обладающий паролем администратора, может легко скомпрометировать данные, хранящиеся и обрабатываемые в данной системе. Следует также отметить, что многие производители систем «Клиент-Банк», уделяющие внимание вопросам ИБ, также требуют запрета удаленного доступа.

Степень риска – высокая.

Были найдены избыточные права

Описание недостатка

На текущий момент многие пользователи информационных систем Компании работают под учетными записями с правами локального администратора (например, сотрудники бухгалтерии).

Описание выявленного риска

Наличие прав локального администратора позволяет пользователю самостоятельно изменять функционал информационной системы, снижая тем самым ее защищенность. В частности, права локального администратора позволяют устанавливать ПО, которое может быть использовано для компрометации других информационных систем.

Степень риска – высокая.

Совмещение критичных сервисов на одном сервере

Описание недостатка

Почтовый сервер одновременно выполняет функции внутреннего DNS-сервера, почтового сервера и контроллера домена.

Описание выявленного риска

Контроллер домена также является почтовым и DNS-сервером, что создает дополнительные угрозы ИБ. В случае же компрометации контроллера домена будет получен доступ ко всем учетным записям и, следовательно, ко всем системам, использующим эти учетные записи. Кроме того, отказ этого сервера повлечет за собой нарушение работоспособности сразу трех ключевых сервисов, а, следовательно, недоступность системы «Клиент-Банк».

Степень риска – средняя.

Было обнаружено, что компания использует децентрализованное управление антивирусной защитой и возможность несанкционированного изменения настроек антивирусной защиты и ее отключения

Описание недостатка

На всех системах в контуре «Клиент-Банк» используются средства антивирусной защиты. Управление осуществляется децентрализованно, централизованной консоли управления и внутреннего сервера обновлений баз антивирусных сигнатур нет, поэтому антивирусное ПО получает обновления напрямую через сеть Интернет с серверов производителя. Антивирусная защита обеспечивает активную защиту в режиме реального времени, защиту электронной почты; настройки обеспечивают автоматическое ежедневное обновление, периодическое полное сканирование настройками не обеспечивается. Полное сканирование производится вручную в случае возникновения нештатных ситуаций (таких как вирусное заражение). Следует также отметить, что пароль, защищающий от несанкционированного изменения настроек антивирусного ПО, не установлен.

Описание выявленного риска

Децентрализованная система управления не позволяет эффективно контролировать антивирусную защиту, а именно лишает возможности видеть целостную картину по отчетам, централизованно изменять настройки, а также организовать централизованный сервер обновлений. Отказ от проведения полного сканирования на периодической основе несет дополнительные риски вирусного заражения, так как при полном сканировании используются расширенные механизмы анализа.

Отсутствие пароля, защищающего от несанкционированного изменения настроек антивирусного ПО, вкупе с децентрализованным управлением создает риски того, что антивирусная защита на отдельных АРМ может быть отключена.

Степень риска – средняя.

Возможности для атаки

- отсутствует комплексный подход к обеспечению информационной безопасности;
- в штате отсутствуют сотрудники, ответственные за информационную безопасность.

Не определены их роли и ответственность;

– акцентирование защитных средств и мер на системах защиты периметра сети. При существующих мерах контроля доступа в сети любое проникновение через внешний защитный периметр Компании способно привести к полной компрометации АСУ ТП;

– в применяемых в АСУ ТП контроллерах ABB Freelance, Motorola MOSCAD и DECONT не используются защитные механизмы. Ни один из используемых в указанных контроллерах протоколах не поддерживается шифрование, аутентификация или авторизация, что позволяет злоумышленнику получить несанкционированный доступ к устройству, информации в нем и иметь возможность удаленно осуществить остановку, перезапуск контроллера, модификацию программы запущенной на нем.

– отсутствует зона DMZ для подключения удаленных пользователей через VPN, что снижает меры контроля при доступе к компонентам АСУ ТП;

– отсутствует зона DMZ между технологической сетью и корпоративной, что повышает риск проникновения в технологическую сеть при компрометации компонентов АСУ ТП, находящихся в сети ЦДП;

– отсутствуют системы IDS на границах с сетью Интернет и в точке межсетевого взаимодействия технологической и корпоративной сети, что не позволяет регистрировать атаки на компоненты АСУ ТП и своевременно реагировать на попытки проникновения в критичные сегменты Компании;

– отсутствует корректное разделение между корпоративной и технологической сетью, некорректно настроена сегментация и межсетевое экранирование на сетевом оборудовании;

– отсутствует перечень всех разрешенных сервисов, протоколов и портов. Отсутствие данного перечня и процесса пересмотра правил на межсетевых экранах в соответствии с данным перечнем часто приводит к тому, что в правилах межсетевых экранов остаются открытыми небезопасные сервисы, что может привести к компрометации компонентов АСУ ТП;

– для управления сетевым оборудованием используется небезопасный протокол telnet, данный протокол передает аутентификационные данные в открытом виде, которые может перехватить злоумышленник при анализе трафика;

– отсутствует должный уровень защиты на серверах системы управления комплексом GENESIS32 на уровне операционных систем (нарушения при использовании учетных записей и паролей). На серверах используются простые неразделяемые учетные записи с административными правами, уязвимые к атакам подбора паролей;

– регулярное обновление системного ПО, прикладного ПО и ПО на ПЛК не осуществляется. Отсутствуют процедуры управления уязвимостями. Данный недостаток не позволяет эффективно контролировать появление общеизвестных уязвимостей в ПО и наличие

небезопасных настроек на ресурсах АСУ ТП для оперативного устранения их. Результатом отсутствия данного процесса в Компании может быть наличие на ряде ресурсов (ПЛК, серверах, АРМ диспетчеров и т.п.) общеизвестных уязвимостей, позволяющих получить полный несанкционированный административный контроль над ними;

– отсутствует процедура управления изменениями. Отсутствие должного контроля за изменениями может привести к нарушению базовых защитных мер информационной инфраструктуры. Это особенно критично с учетом частых изменений в информационной инфраструктуре Компании;

– отсутствует должный уровень защиты на серверах системы управления комплекса GENESIS32 на уровне прикладного ПО GENESIS32 (недостатки в реализации парольной политики, недостатки в реализации разграничения доступа в АСУ ТП, недостатки в реализации сетевого доступа к серверам АСУ ТП). Текущая реализация процессов управления доступом пользователей позволяет формировать пользовательские учетные записи с паролями, уязвимыми к атакам подбора. Кроме того, существующий процесс не гарантирует своевременной блокировки учетных записей пользователей при их увольнении;

– антивирусная защита серверов и рабочих мест АСУ ТП осуществляется не в полном объеме;

– отсутствуют процедуры мониторинга событий информационной безопасности и реагирования на инциденты. Отсутствуют системы сбора и анализа событий информационной безопасности, что не позволяет вовремя выявлять действия злоумышленников и противодействовать им;

– отсутствуют средства анализа защищённости ресурсов АСУ ТП;

– в АСУ ТП применяются средства защиты, не прошедшие в установленном порядке оценку соответствия;

– отсутствует процедура повышения осведомленности пользователей в вопросах информационной безопасности. Неосведомленность пользователей в вопросах ИБ может быть использована злоумышленниками для проведения атак методом социальной инженерии.

Кроме того, в Компании не реализован процесс управления рисками, что не позволяет эффективно направлять усилия по обеспечению информационной безопасности и обеспечивать соответствие реализованных защитных мер существующим угрозам.