ОБЩЕСТВЕННАЯ ОРГАНИЗАЦИЯ
«ВСЕУКРАИНСКОЕ ОБЪЕДИНЕНИЕ СПЕЦИАЛИСТОВ БЕЗОПАСНОСТИ»
Идентификационный код юридической особы 40346769

Часть №1

АНАЛИТИЧЕСКАЯ СПРАВКА

криптостойкость и имитостойкость охранного оборудования и систем.

В соответствии с многочисленными обращениями от членов и партнеров нашего объединения нами, с привлечением специалистов производителей и официальных представителей, предприятий охраны (пульт), изучался вопрос и обобщались сведения по нему, а именно:

«КАКИЕ СУЩЕСТВУЮТ АППАРАТНЫЕ, ТЕХНИЧЕСКИЕ, ОРГАНИЗАЦИОННЫЕ И ДРУГИЕ СПОСОБЫ И МЕТОДЫ ЗАЩИТЫ ОТ ВОЗМОЖНОСТИ «ПОДМЕНЫ» ОБЪЕКТОВЫХ ПРИБОРОВ (ППК) С ЦЕЛЬЮ ПРОНИКНОВЕНИЯ НА ОХРАНЯЕМЫЙ ОБЪЕКТ В ЭКСПЛУАТИРУЕМЫХ СИСТЕМАХ/ПУЛЬТАХ ЦЕНТРАЛИЗОВАННОГО НАБЛЮДЕНИЯ (ПЦН)».

Были рассмотрены следующие системы централизованного наблюдения.

- ПЦН «МОСТ» и ППК «ОРИОН», производитель ООО «Тирас – 12».

- ПЦН «ОРЛАН» и ППК «ЛУНЬ», производитель ООО «Охрана и Безопасность».

- ПЦН «ГЕРМЕС» и ППК «МАКС», производитель ООО «ITV».

- ППК производителя ООО «НПФ АЯКС».

- ПЦН и ППК производителя «PIMA», представитель ООО «РМ Системс».

- ПЦН «STAM» и ППК производителя «Satel», представитель ООО «Дифенс».

- ПЦН и ППК производителя «Jablotron», представитель ООО «Яблотрон Украина».

Данный список составлен согласно информации от предприятий и специалистов безопасности, которые являются членами или партнерами нашей организации. При желании других производителей или поставщиков мы можем добавить соответствующий раздел.

ОПРЕДЕЛЯЮЩИЕ ТЕРМИНЫ.

"Криптостойкость" (интеллектуальный саботаж - подмена данных, атака ManInTheMiddle) - способность криптографического алгоритма противостоять криптоанализу. Стойким считается алгоритм, успешная атака на который требует от атакующего обладания недостижимым на практике объёмом вычислительных ресурсов или перехваченных открытых и зашифрованных сообщений либо настолько значительных затрат времени на раскрытие, что к его моменту защищённая информация утратит свою актуальность. В большинстве случаев криптостойкость не может быть математически доказана; можно только доказать уязвимости криптографического алгоритма либо (в случае криптосистем с открытым ключом) свести задачу взлома алгоритма к некоторой задаче, которая считается вычислительно сложной (то есть доказать, что взлом не легче решения этой задачи).

"Имитостойкость" (подмена ППК) - свойство криптографической системы или криптографического протокола, характеризующее способность противостоять активным атакам со стороны противника и/или нарушителя, целью которых является навязывание ложного сообщения, подмена передаваемого сообщения или изменение хранимых данных.

ПРИМЕР.

В поле зрения преступников попал частный дом в одном из пригородных поселков «N».

Хозяева частенько уезжают заграницу и сдают дом под сигнализацию на пульт охраны.

Отметим, что данная преступная группировка обладала и финансовым, и материальным потенциалом, и технически подготовленными специалистами- знакомыми с особенностями оборудования и систем сигнализации.

Путем «оперативно – изыскательских» действий данные преступники получают следующую информацию об интересуемом объекте и системе охранной сигнализации, которая задействована для его технической охраны:

- наименование предприятия (подразделение), которое осуществляет охрану данного объекта.
- тип приемо – контрольного прибора, установленного на объекте.
- схему расположения датчиков охранной сигнализации.
- канал(ы) передачи информации от приемо – контрольного прибора на систему централизованного наблюдения (пульт охраны).
- каким оператором связи пользуется пульт охраны для данной системы.

Одними из выясненных преступниками особенностей было отсутствие блокировки помещения на втором этаже (детская спальня) и то, что приемо – контрольный прибор был расположен в нише щитовой на лестнице между 1-ым и 2-ым этажами. Хочется отметить, что ОЧЕНЬ многие клиенты с целью экономии и др. причин отказываются от блокировки не только окон, но и помещений (датчики движения) 2-го и выше этажей.

Затем были сделаны пробные «сработки» средств сигнализации на данном объекте с целью определения действий сотрудников группы реагирования.

В одну из ночей, когда хозяева дома уехали заграницу, к дому подошли три человека с раскладной лестницей и путем нехитрого отжима металлопластикового окна один из них залез в помещение детской спальни. Плотно закрыв окно, он подождал, пока его напарники уйдут на безопасное расстояние и подадут ему команду для дальнейшего ключевого действия.

Быстро спустившись к нише, он вырвал антенну и запитал через рядом имеющуюся розетку некий «черный ящик».

Что же происходило на пульте охраны?

В 01.45 в частном доме пригородного поселка «N» сработал датчик коридора 2-го этажа. Срабатывание было единичное. Опрос прибора через 2 минуты показал по всем зонам прибора «норму». Дежурный пульта принимает решение группу не посылать.

Можем отметить, что если бы группа реагирования прибыла на объект и не обнаружила бы следов проникновения (а их не было), то с вероятностью 95% никто бы доверенных лиц не вызывал и объект не перезакрывал бы.

Выждав 40 минут, подельники присоединились к своему первому лицу и начали паковать вещи, бытовую технику и пр. материальные ценности.

В результате «профессиональных» действий преступников, непрофессионального подхода сотрудников службы охраны и «экономии» хозяев, по приезду из заграницы их ждал неприятный сюрприз.

Данный пример вымышлено – собирательный, но, на наш взгляд, вполне реальный.

Основным действующим неодушевленным лицом в данной истории является «черный ящик». Это такой же приемо – контрольный прибор (почти 100% «клон»), который имитировал техническую охрану данного дома во время ограбления.

Что же может предотвратить подобную ситуацию, а именно - создания и использования такого «черного ящика»?

Вот что рекомендуют производители наиболее распространенных в Украине технических систем охраны.

ОБОБЩЕННЫЕ ОТВЕТЫ И РЕКОМЕНДАЦИИ

Производитель - Компания «Тирас - 12» (Украина)
СЦН «Мост», ПО «Мост», ППК серии «Орион».

Согласно ответа производителя ООО «Тирас – 12», за подписью технического директора Кононко А.Н., данные функции по "имитостойкость" и "криптостойкость" обеспечиваются следующим функционалом.

Для предотвращения саботажа со стороны злоумышленника в приемно-контрольных приборах (ПКП) предусмотрены следующие аппаратные, технические и программные меры:

- защиту от проникновения в корпус прибора или его составных частей обеспечивается тамперной зоной, которую необходимо контролировать (круглосуточно);
- связь прибора с его составляющими частями и пультом централизованного наблюдения (далее ПЦН) постоянно контролируется и нарушение его передается на прибор и ПЦН;
- наличие криптозащищенного протокола между составными частями прибора и ПЦН обеспечивает защиту от подмены составных частей и прибора с помощью уникальных идентификационных кодов (скрытые номера);
- на случай умышленного обесточивания объекта в приборе предусмотрено резервное питание от аккумулятора;
- номинал оконечного резистора не позволяет блокировать шлейф сигнализации прибора дополнительным или параллельным резистором.

Пользователям, Инсталяторам, Обслуживающему персоналу ПКП необходимо предусмотреть следующие организационные мероприятия:

- исключить блокировку тамперной зоны прибора и его составных частей технологическими перемычками;
- не располагать оконечные резисторы шлейфов сигнализации в корпусе прибора;
- не располагать трансивер и антенну ПКП на объекте охраны в легкодоступном месте или вне охраняемого помещения;
- максимально ограничить доступ к кодам доступа пользователей, администратора, разработчика;
- не допускать эксплуатирование ПКП без аккумулятора;
- своевременно, после вмешательства технического специалиста пультовой организации в прибор, менять коды доступа пользователям на другие;
- резервировать канал связи прибора с ПЦН с помощью 2-й SIM карты и модуля для подключения к сети Ethernet («БПМЕ», «M-NET»);
- дублировать сообщения, которые передаются от прибора на ПЦН посредством SMS сообщений владельцу объекта;
- настраивать функцию прибора «Активации реагирования сразу при нарушении входных дверей без ожидания завершения задержки на вход» (подробно описано в паспорте на соответствующий прибор).

Администраторам ПЦН необходимо предусмотреть следующие организационные мероприятия на пультах:

- при настройке пультового оборудования обеспечивать наличие альтернативного IPадреса (на другом провайдере услуг Internet);
- придерживаться требований производителя относительно нагрузки Ethernet-порта на ПЦН;
- придерживаться требований производителя относительно общей нагрузки ПЦН объектами наблюдения и своевременно расширять под серверную систему;
- «время контроля тестовых сообщений от прибора» в карточке объекта на ПЦН рекомендуется устанавливать в несколько раз больше, чем «интервал передачи тестовых сообщений на ПЦН» в приборе;
- для обеспечения достаточной скорости ПЦН использовать накопитель типа SSDв компьютере, на котором установлено пультовое программное обеспечение.

Производитель - Компания «Охрана и Безопасность» (Украина)
СЦН «Орлан», ПО «Феникс 4», ППК серии «Лунь».

Согласно ответа изготовителя ООО «Охрана и Безопасность», за подписью Директора Чернышева С.Н., данные функции по "имитостойкость" и "криптостойкость" обеспечиваются следующим функционалом.

- При использовании голосового канала передачи информации (GSM, CSD, SMS) контроль ППК обеспечивается его сим-картой (тел. номер).
- При использовании канала передачи информации мобильный интернет (GPRS) контроль ППК обеспечивается его статическим IP в приделах VPN сети (не путать с публичными IP).
- Основным способом защиты от подмены ППК является использование закрытой VPN-сети предоставляемой оператором мобильной связи (Киевстар, МТС, Lifecell). В эту сеть нет доступа из Интернет или других закрытых сетей. Данный способ позволяет практически

исключить возможность подмены оборудования, при условии ограничения доступа к управлению сим-картами, использование сим-пар и т.д. и свести их до одного - двух ответственных сотрудников.

- Также при использовании открытого интернета можно обеспечить защиту передаваемого номера защитив конфигурацию ППК «Лунь 11», «Лунь 19», «Лунь 23» паролем, но это не спасает от "подсматривания" передаваемого номера в базе пульта.

Производитель - Компания «Integrated Technical Vision Ltd.» СЦН «Гермес», ПО «Мониторинг III», ППК серии «Макс».

Согласно ответа изготовителя ООО «Integrated Technical Vision Ltd.», согласованного с Техническим директором Суярко А.Ю., данные функции изначально закладывались ими в ППК и СЦН (приемники, конвертеры и программное обеспечение) при их разработке, а именно.

"Имитостойкость" и "криптостойкость" обмена данными обеспечивается так:

1. Шифрование пакета данных (256-битный ключ). В зашифрованной области содержатся: заводской номер устройства, идентификатор пакета данных, пультовой номер ППК.
2. **Контроль уникального заводского номера устройства - GID (передается в пакете данных).**
3. Контроль идентификаторов пакетов данных (защита от повторной отправки тех же данных).
4. Контроль пультового номера ППК.
5. Контроль телефонного номера ППК (дополнительный пункт контроля в ПЦН Гермес, при работе по GSM).

Кроме этого, обеспечивается резервирование и контроль канала связи посредством периодических тестовых сигналов.

Максимальная устойчивость ко взлому, саботажу и искажению передаваемых данных обеспечивается в следующих протоколах ITV: TCP GPRS, UDP GPRS, Ethernet, Bell110 (GSM дозвон), CSD (GSM дозвон), SMS (GSM), Bell110 (дозвон по тел. линии).

Также возможна работа в закрытых VPN сетях (GPRS VPN - в которых оператор обеспечивает недоступность ППК извне) при использовании ПС МАКС GPRS или с помощью роутера с 3G модемом для остальных СЦП.

По взаимодействию ППК и СЦН

При использовании ПЦН «Гермес» и ПО «Мониторинг III»

Прямой прием извещений от ППК в протоколах TCP GPRS, UDP GPRS, Ethernet и от ПЦН Гермес в Ethernet.

При обнаружении подмены ППК генерируется соответствующее тревожное событие, для оповещения и обработки оператором.

С помощью ПЦН Гермес прием в протоколах UDP GPRS, Ethernet, Bell110 (GSM дозвон), CSD (GSM дозвон), SMS (GSM), Bell110 (дозвон по тел. линии).

Данные о серийных номерах ППК и их телефоны в ПЦН Гермес загружаются из ПО Мониторинг III.

При обнаружении подмены ППК - несоответствии серийного номера/аккаунта/телефонного номера(GSM), а также звонка с неизвестного телефонного номера генерируются соответствующие тревожные события для передачи в ПО Мониторинг, для оповещения и обработки

оператором.

В данной конфигурации так же возможна поддержка закрытых VPN сетей (GPRS VPN) при использовании роутера с 3G модемом/3G модема.

При использовании ПЦН Гермес в варианте интеграция по ContactID с пультовым ПО других производителей.

Прием в протоколах UDP GPRS, Ethernet, Bell110 (GSM дозвон), CSD (GSM дозвон), SMS (GSM), Bell110 (дозвон по тел. линии).

Данные о серийных номерах ППК и их телефоны загружаются с помощью ПО Ess.Hardware.Tools (Конфигуратор). Передача данных в пультовое ПО - по RS232. Есть возможность работать одновременно в составе Мониторинг III (по Ethernet) и с пультовым ПО других производителей одновременно.

При обнаружении подмены ППК - несоответствии серийного номера/аккаунта/телефонного номера(GSM), а также звонка с неизвестного телефонного номера генерируются соответствующие тревожные события для передачи в пультовое ПО, для оповещения и обработки оператором.

Возможно использование команд (реконфигурация, смена прошивки) с пульта. Они отправляются с помощью утилиты Ess.Hardware.Tools.

В данной конфигурации так же возможна поддержка закрытых VPN сетей (GPRS VPN) при использовании роутера с 3G модемом.

При использовании ПС «Макс GPRS», интеграция по ContactID с пультовым ПО других производителей.

Прием в протоколах UDP GPRS, Ethernet, Bell110 (GSM дозвон), CSD (GSM дозвон).

Возможна непосредственная поддержка закрытых VPN сетей (GPRS VPN), в которых оператор обеспечивает недоступность ППК извне.

Приемник не требует явного внесения учетной записи объекта (серийный номер, аккаунт) в базу данных (память) приемника. Учетная запись ППК в базе приемника автоматически создается после первого принятого извещения от ППК, из которого извлекается GID и аккаунт.

Первая полученная учетная запись считается правильной и корректной.

При обнаружении подмены ППК - несоответствии серийного номера и аккаунта - генерируются соответствующие тревожные события для передачи в пультовое ПО, для оповещения и обработки оператором.

Если это была санкционированная замена оборудования на объекте с сохранением пультового номера (аккаунта), то с помощью ПО Ess.Hardware.Tools можно удалить старую запись из базы приемника - на её месте автоматически создастся новая.

Дубликат удалится и извещение "Саботаж" по этому объекту больше приходить не будет, **объект в пределах приемника станет уникальным.**

Передача данных в пультовое ПО - по USB. При подключении приемника создаются 2 COM порта - один для передачи данных в пультовое ПО, второй - для использования команд с пульта (опрос, перевзятие группы, взятие группы, реконфигурация, смена прошивки) с пульта.

Управление приемником - просмотр базы аккаунтов, событий, отправка команд – происходит с помощью утилиты Ess.Hardware.Tools.

При использовании ПС «Макс Ethertnet», интеграция по ContactID с пультовым ПО других производителей

Прием в протоколах UDP GPRS, Ethernet.

Возможна поддержка закрытых VPN сетей (GPRS VPN) при использовании роутера с 3G модемом.

Приемник не требует явного внесения учетной записи объекта (серийный номер, аккаунт) в базу данных (память) приемника. Учетная запись ППК в базе приемника автоматически создается после первого принятого извещения от ППК, из которого извлекается GID и аккаунт.

Первая полученная учетная запись считается правильной и корректной.

При обнаружении подмены ППК - несоответствии серийного номера и аккаунта - генерируются соответствующие тревожные события для передачи в пультовое ПО, для оповещения и обработки оператором.

Если это была санкционированная замена оборудования на объекте с сохранением пультового номера (аккаунта), то с помощью ПО Ess.Hardware.Tools можно удалить старую запись из базы приемника - на её месте автоматически создастся новая.

Дубликат удалится и извещение "Саботаж" по этому объекту больше приходить не будет, объект в пределах приемника станет уникальным.

Передача данных в пультовое ПО - по USB. При подключении приемника создаются 2 COM порта - один для передачи данных в пультовое ПО, второй - для использования команд с пульта (опрос, перевзятие группы, взятие группы, реконфигурация, смена прошивки) с пульта.

Управление приемником - просмотр базы аккаунтов, событий, отправка команд - с помощью утилиты Ess.Hardware.Tools.

Все вышеперечисленные особенности по имитостойкости и криптозищите оборудования можно найти в презентации на официальном сайте производителя и на каждом диске, поставляемом с изделиями производителя.

Так же в ПО «Мониторинг III» возможна привязка и контроль статических IP адресов ППК, но по рекомендации производителя она не рекомендуется и вот почему:

От данной практики и рекомендаций производитель отказался, так как IP адрес не является защищенным от подмены в IP протоколах, а привязка к статическим IP приводит к дополнительной нагрузке при настройке объекта на инженеров пульта.

При смене конфигурации сетей на стороне оператора связи можно получить либо не работающую систему, либо систему с большим количеством ложных извещений о саботаже устройств.

Если же злоумышленник получит доступ к такой сети с фиксированными IP (утечка SIM карт и т.д.), он сможет заниматься саботажем, или блокировать приборы с помощью DDoS атак.

Поэтому ППК «Макс» и СЦН «Гермес» разрабатывались так, чтобы работать в сетях со сложной, динамически изменяемой топологией. Основой технологии есть клиент-серверная модель и нотификационная схема работы - ППК является клиентом, а СЦН сервером. Идентификатором ППК является заводской серийный номер прибора, дополнительно защищенный шифрованием.

Данная технология позволяет работать ППК так, что данные беспрепятственно проходят через различные NAT-ы (Network address translation), без дополнительной настройки на сетевом оборудовании. В то же время NAT-ы на маршрутизаторах дают дополнительную степень защиты, позволяя обмен данными только по установленному ППК соединению с сервером (идентификатор - пара IP адрес и порт ППК/IP адрес и порт сервера), исключая вмешательство третьих лиц.

После приема пакета данных от ППК, СЦН получает IP адрес и порт прибора, и может отправлять как пакеты подтверждения приема, так и обратные команды (опрос, подтверждение постановки, перепостановка, удаленное взятие, вычитка и загрузка микропрограммы, команда обновления микропрограммы по FTP).

Значение IP адреса и порта прибора в СЦН обновляются при каждом приеме данных от ППК. Таким образом, если адрес ППК в сети будет изменен (изменение топологии оператором, уход от flood атаки или переход на другую SIM карту) то прибор останется на связи.

По сравнению с опросной технологией (когда сервер должен знать IP адреса устройств, чтобы периодически их опрашивать) клиент-серверная технология требует меньше ресурсов сервера и позволяет повысить скорость приема извещений.

Производитель - Компания «НПФ АЯКС» (Украина)
ППК серии «Ajax Hub».

Согласно ответа производителя ООО «НПФ Аякс», за подписью директора Конотопского А._, функции по "имитостойкости" и "криптостойкости" в ППК и других составляющих предусмотрено следующими мероприятиями:

- Передача данных зашифрована, с использованием алгоритма шифрования AEC128.
- Проверка оригинальности ППК «Ajax Hub» производится уникальным ID и программным обеспечением, которое предоставляется производителем для сторонних СЦН.
- Передача данных сторонним СЦН происходит в протоколе «Contact ID».
- Для получения данных от ППК «Ajax Hub» до сервера СЦН производитель предоставляет программное обеспечение, которое получает информацию в зашифрованном виде и только потом конвертируется в «Contact ID». При этом за целостность пакетов в протоколе «Contact ID», гарантию их доставки внутри локальной инфраструктуры СЦН отвечает инженерно технический персонал предприятия охраны.

Следует отметить, что специалисты предприятия производителя пояснили, что у них нет собственной системы централизованного наблюдения и поэтому оборудование (ППК «Ajax Hub») адаптировано к работе со сторонними СЦН такими как «Орлан» (ПО «Феникс»).

Производитель - Компания «PIMA Electronic Systems» (Израиль)
СЦН и ППК производства «Pima».

Согласно ответа официального представителя ООО «РМ Системс», за подписью Директора Романенка С.Н., данные функции по "имитостойкость" и "криптостойкость" обеспечиваются следующим функционалом но при этом не являются технической документацией.

Исходная иформация - (номер объекта, код события, номер группы/зоны и т.д.)

Формат центральной станции (далее кодирующий ключ) - по сути является идентификатором ключа - указатель на *ключ,* представляющий собой системное имя ключа в программной реализации *криптографического алгоритма* и имеющий установленный в системе формат. Используется в качестве переменной при записи различных *криптографических операций* в тексте программы.

В зависимости от используемых каналов связи, используются различные способы защиты сообщений от несанкционированного прочтения и доступа к исходной информации:

Общее для всех каналов передачи PIMA Electronic Systems:

Расшифровка исходной информации возможна исключительно при наличии правильного ключа и алгоритма протокола передачи данных, а также с использованием приемной аппаратуры производства PIMA Electronic Systems.

Перечень кодирующих ключей всех производимых PIMA Electronic Systems ПЦН, их местонахождение, изготовленные драйвера, являются коммерческой тайной PIMA Electronic Systems и не подлежат разглашению.

Для уменьшения человеческого фактора, введена функция при которой передача сообщений с ППКОП без ввода кодирующего ключа невозможна.

Считать параметры ППКОП через программатор и программу конфигурирования с прибора возможно только тем же экземпляром программы и с кодом загрузки и считывания, с которым этот ППКОП был запрограммирован.

Без указания кодов считывания и кодов загрузки программа конфигурирования позволит записать новые данные, но прочитать уже записанные данные на объекте невозможно.

Привязка драйверов и кодирующих ключей к конкретным владельцам ПЦН известна только официальным представителям PIMA Electronic Systems в конкретном регионе/стране и не известна производителю.

Защита информации об используемом ключе на конкретном экземпляре ПЦН достигается организационными мерами и передается производителем руководству ПЦН совместно с методическими указаниями.

1. При использовании телефонной линии и автодозвонного типа связи:

Каждое сообщение представляет собой измененную исходную информацию, зашифрованную с помощью кодирующего ключа, а также с использованием закрытых типов протоколов производителя, не подлежащие разглашению (PAF/NPAF/EPAF/PID).

Таким образом начальная информация защищается двумя составляющими:

- вводом ключа в аппаратуру на объекте охраны (ППКОП) и наличием данного ключа на пульте централизованной охраны (ПЦН), которые являются уникальными для каждого ПЦН, производимого PIMA Electronic Systems и программируется производителем для каждого ПЦН персонально;
- унитарными протоколами передачи, стойкими к декодированию (PAF/NPAF/EPAF/PID).

Так как часть технических работников пульта имеют информацию о ключе, который используется на данном конкретном ПЦН, при использовании ППКОП PIMA Electronic Systems, они смогут имитировать передачу идентичного сообщения с другого ППКОП на этот ПЦН.

Однако передать и имитировать сообщение на другие ПЦН PIMA Electronic Systems, не зная ключа другого ПЦН и не имея драйвера для приемной аппаратуры ПЦН, технически невозможно.

Поэтому необходимо организовать учет ППКОП с прошитыми ключами и исключить их наличие у других лиц (бывший Клиент, Инсталятор и пр.).

2. При использовании радиоканала большого радиуса действия:

Каждое сообщение представляет собой измененную исходную информацию (номер объекта, код события, номер группы/зоны и т.д.), зашифрованную с помощью кодирующего ключа, а также с использованием закрытых типов протоколов производителя, не подлежащие разглашению(PAF/NPAF/EPAF/PID).

Таким образом, начальная информация защищается следующими составляющими:

- вводом ключа в аппаратуру на объекте охраны (ППКОП) и наличием данного ключа на пульте охраны (ПЦН), которые являются уникальными для каждого ПЦН, производимого PIMA Electronic Systems и программируется производителем для каждого ПЦН персонально;
- унитарными протоколами передачи, стойкими к декодированию (PAF/NPAF/EPAF/PID);
- использованием в протоколе передачи фазочастотной модуляци сигнала (ФЧМ);
- использованием собственных выделенных частот передачи сигнала.

Так как часть технических работников пульта имеют информацию о ключе, который используется на данном конкретном ПЦН, зная рабочую частоту конкретного ПЦН, при использовании ППКОП PIMA Electronic Systems с радиопередатчиком конкретного диапазона, они смогут имитировать передачу идентичного сообщения с другого ППКОП на этот ПЦН.

Однако передать и имитировать сообщение на другие ПЦН PIMA Electronic Systems, не зная ключа другого ПЦН и не имея драйвера для приемной аппаратуры ПЦН от производителя, технически невозможно.

Поэтому необходимо организовать учет приемо-передающих устройств и ППКОП с прошитыми ключами и исключить их наличие у

других лиц (бывший Клиент, Инсталятор и пр.).

3. При использовании каналов GSM (GPRS) , а так же Интернет (WAN/LAN)

Каждое сообщение представляет собой измененную исходную информацию (номер объекта, код события, номер группы/зоны и т.д.), зашифрованную с помощью, алгоритма шифрования AES (*Advanced Encryption Standard (AES), также известный как Rijndael— симметричный алгоритм блочного шифрования…*) с длинной ключа 256 бит, а также с использованием закрытых типов протоколов производителя, не подлежащие разглашению.

Для защиты от возможного саботажа или подмены ППКОП, реализована функция подсчета всех сообщений от каждого ППКОП по принципу count (прибор присваивает сообщениям номер, а ПЦН считает данные сообщения) с программным контролем на ПЦН.

Данный признак номера шифруется по алгоритму AES 256 бит вместе с телом исходного сообщения и декодируется с помощью ключа со стороны ПЦН.

В упрощенном варианте это выглядит так:

- если ППКОП передает сообщение с присвоенным номером 255, а ПЦН ожидает сообщение 1344 от данного объектового номера, программа выдаст сообщение о попытке подмены ППКОП.

Формирование ключа длинной 256 бит производится из вводимой в ППКОП и ПЦН последовательности из 64 байт по определенному алгоритму.

Также в программном обеспечении есть функция фильтрации IP адресов и привязки объектовых номеров к конкретным IP, но на большинстве ПЦН на территории стран бывшего СНГ этот функционал не используется.

Таким образом начальная информация защищается следующими составляющими:

- использованием алгоритма шифрования AES 256 бит;
- вводом ключа 256 бит в аппаратуру на объекте охраны (ППКОП) и наличием данного ключа на пульте охраны (ПЦН), и программируется для каждого ПЦН персонально техническим персоналом ПЦН;
-использованием функции подсчета сообщений count;
- унитарными протоколами передачи данных, стойкими к декодированию;

Так как часть технических работников пульта имеют информацию о ключе, который используется на данном конкретном ПЦН, при использовании ППКОП PIMA Electronic Systems, они смогут передать идентичное сообщения с другого ППКОП на этот ПЦН, однако не смогут обойти счетчик сообщений и система выдаст сообщение о подмене ППКОП.

Также в Украине используются устройства передачи по каналу GSM-GPRS (коммуникаторы «ISI-GPRS) на СЦН «Pima», для переключения ППКОП другого производителя, работающих в общедоступных протоколах типа Ademco CID.

В данных устройствах реализованы следующие принципы защиты:

- использование алгоритма шифрования AES 128 бит;
- ввод вручную в карту SIM номера телефона, с которого возможно получать СМС с параметрами программирования;
- при первом сеансе святи необходимо подтверждение со стороны ПЦН о подключении нового устройства, после этого ПЦН отправляет кодирующий ключ на коммуникатор для дальнейшего использования в шифрованном виде;
- возможность изменения установленного ключа кодирования одновременно для всех коммуникаторов с повторным подтверждением их подключения на ПЦН;
- ключ шифрования в открытом виде не передается, а кодируется случайным ключом по алгоритму, известным только производителю;

- для защиты от возможного саботажа или подмены ППКОП, в случае повторного запроса ключа от уже существующего в базе подключений коммуникаторов, программное обеспечение выдает сообщение о возможном саботаже, с повторным требованием подтверждения подключения.

Производитель - Компания «Satel» (Польша)
СЦН «Stam», ППК производства «Satel».

Согласно ответа производителя «Satel», за подписью начальника отдела Ярослава Журавик, данные функции по "имитостойкости" и "криптостойкости" в ППК и других составляющих систем и оборудования предусмотрено несколькими уровнями защиты, а именно:

- на этапе производства – это присвоение внутреннего уникального индивидуального серийного номера каждому элементу системы.
- на этапе монтажа – это два процесса, адресация и идентификация как уникальных индивидуальных серийных номеров системы непосредственно ППК, так и контроля внесения изменения в конфигурацию.

«Общение» оборудования в рамках одной системы проходит посредством обмена по внутреннему протоколу собственной разработки компании «Satel». Кроме того выходная трансмисия данных дополнительно кодируется 192-битовым ключом.

Производитель - Компания «Jablotron» (Чехия)
СЦН «», ППК производства «Jablotron».

Согласно ответа официального представителя ООО «Яблотрон Украина», за подписью Коммерческого директора Василия Искакова, оборудование охранного назначения производства «Jablotron» (Чехия) отвечает всем строгим требованиям европейской серии стандартов – EN-50131, степень безопасности второй, класс окружающей среды II. Это подтверждено соответствующими сертификатами как в Чешской Республике, так и в Украине – продукция регулярно проходит обязательную сертификацию в «ГЦССОН» г. Киев.

Что касается раскрытия информации в отношении задействованных методов производителем защиты от подмены ППК и защиты от интеллектуального саботажа – эта информация относится к закрытой и составляет технологическую и коммерческую тайну, которую производитель не разглашает вторым лицам.

Для обеспечения надежной работы оборудования Jablotron по охране имущества различных форм собственности на территории Украины, ООО «Яблотрон Украина», как эксклюзивный представитель Jablotron Alarms в Украине, регулярно проводит учебные семинары-тренинги по подготовке квалифицированных инсталляторов оборудование Jablotron, также мы сотрудничаем как с Полицией Охраны, так и с многими частными Охранными Агентствами.

Отметим, что ООО «Яблотрон Украина» - это единственное предприятие (официальный представитель производителя), который не предоставил конкретных данных и рекомендаций. При этом нами принята позиция Предприятия по ее «коммерческой тайне» и не передачи информации «вторым лицам».

Хотя следует отметить, что почти полное отсутствие нормативной базы в государстве по вопросу защиты объектов техническими средствами охраны и свободную (неконтролируемую) продажу охранного оборудования, данная позиция «коммерческой тайны», к сожалению, не имеет смысла.

Стоит отметить, что все производители, за исключением компаний «ITV» и «Аякс», дали свои рекомендации, исходя из того, что их объектовое оборудование будет работать с их же системами централизованного наблюдения.

Государственный центр сертификации средств охранного назначения Департамента полиции охраны (ГЦС СОН ДПО)

Согласно официального ответа, данного государственным центром сертификации, за подписью начальника центра Грицуника О.Д., устойчивость средств охранного назначения относительно несанкционированного вмешательства регламентируется национальными стандартами.

В частности, относительно приборов приемно – контрольных требования определены в следующих стандартах.

1. **ДСТУ EN 50131-1:2014** Системы тревожной сигнализации. Системы охранной сигнализации.

Часть 1. Общие требования.

Пункт 8.7. Несанкционированное вмешательство: выявление защиту.

Пункт 8.8. Взаимосвязь.

2. **ДСТУ EN 50131-3:2014** Системы тревожной сигнализации. Системы охранной сигнализации.

Часть 3. Приборы приемно - контрольные.

Пункт 8.7. Несанкционированное вмешательство: выявление защиту.

3. **ДСТУ EN 50131-5-3:2014** Системы тревожной сигнализации. Системы охранной сигнализации.

Часть 5-3. Требования к взаимосвязей оборудования с использованием радиочастотных технологий.

Пункт 4.3. Устойчивость к нечаянного и намеренного замещения компонента и сообщения.

4. **ДСТУ EN 50136-2:2014** Системы тревожной сигнализации. Системы передачи тревожных извещений и оборудования.

Часть 2. Требования к трансивера под охранного помещения (ТПП).

Пункт 6.3. Защита от подмены.

Пункт 6.4. Информационная безопасность.

Схемой сертификации средств охранного назначения органа по сертификации ДЦС ООП ДПО предусмотрено проведение оценки соответствия оборудования указанным требованиям согласно **степени его безопасности** и **зависит от конкретного заказа на проведение работ**. *Комментарий – В своем Заказе на сертификацию Производитель – Поставщик сам определяет «степень безопасности» оборудования, перечень и уровень мероприятий по защите его от подмены.*

Требования, по которым оборудование и системы прошли сертификацию в органе по сертификации ДЦС ООП ДПО определены в сертификатах соответствия, выданные заказчикам работ. *Комментарий – В Сертификате, выданном органом сертификации, в разделе «Соответствует требованиям» указываются конкретные требования ДСТУ которым .*

Для информации следует добавить, что Согласно терминологии «ДСТУ EN 50131-1, Системы тревожной сигнализации, Системы охранной сигнализации».

Часть 1.Общие требования.

«Классификация (безопасности систем охранной сигнализации) должна соответствовать одному из четырех классов, 1 класс является основным классом, а класс 4 - самым высоким.

Для системы спецификаторов (*центров сертификации*), которые отвечают за безопасность помещения, устанавливаются следующие классы:

«**Класс 1**: Низкая степень риска

Предполагается, что злоумышленники будут иметь низкий уровень знаний систем охранной сигнализации и будут ограничены диапазоном легкодоступных инструментальных средств.

Класс 2: Низко - средняя степень риска.

Ожидается, что злоумышленники будут иметь ограниченное знание систем охранной сигнализации и будут использовать обычный диапазон инструментальных средств и портативных инструментов.

Класс 3: Высоко - средняя степень риска.

Ожидается, что злоумышленники будут ознакомленными с системами охранной сигнализации и будут использовать большой диапазон инструментальных средств и портативного электронного оборудования.

Класс 4: Высокая степень риска.

Используется, когда безопасность имеет приоритет над всеми другими показателями. Ожидается, что злоумышленники будут иметь возможность или ресурс для того, чтобы подробно планировать вторжения, и будут иметь весь необходимый ряд оборудования, включая средства подстановки жизненно важных компонентов в системе охранной сигнализации.»

Существенным добавлением к данной информации о системе классификации (ДСТУ EN 50131-1) следует отметить тот факт, что из проверенных Сертификатов вышеперечисленных производителей все Приборы Приемо – Контрольные и другое сопутствующее оборудование имеет Класс степени безопасности не выше 2.

Советы

Рекомендуем руководителям, лицензиату и собственникам предприятий охраны:

- Лично провести (присутствовать) самостоятельные испытания по осуществлению «подмены» объектового оборудования на своих пультах охраны с использованием принятых на них методов «подключения» приборов охраны к системам централизованного наблюдения.
- Проверить выполнение рекомендованных мероприятий на охраняемых объектах, правильность и полноту их блокировки техническими средствами охраны.
- Проанализировать организационные мероприятия по «защите» основных каналов передачи информации.
- Вникнуть в разрешительную (Сертификаты) и техническую (Инструкции) документацию закупаемого оборудования. Посмотреть, какие параметры были проверены и сертифицированы органом сертификации.

Некоторые результаты и выводы.

1. К сожалению, по нашим данным, полученными в ходе опроса, очень мало пультов охраны используют рекомендуемые производителем методы «защиты» в полном объеме. Некоторые пульты в ходе изучения данной темы с невероятной легкостью провели «подмену» объектового оборудования даже с полным выполнением рекомендованных мероприятий.

2. Сами «методы защиты», которые производители заложили в свое оборудования или рекомендуют выполнять, во многом, а в некоторых случаях полностью, зависят от сотрудников охраны или монтажных организаций.

3. В большинстве своем (по разным причинам) специалисты пультов охраны работают по упрощенным схемам, которые в основном опираются на человеческий фактор и тем самым значительно увеличивают вероятность «профессиональной» кражи или разбоя на охраняемом объекте.

4. Очень часто монтажом технических средств безопасности занимаются люди, которые имеют о данном оборудовании и о способах защиты лишь поверхностное представление.

5. Многие объекты, особенно квартиры, частные дома оборудуются по придуманным неквалифицированными специалистами типовым схемам. Так как ни на государственном, ни на общественном уровне данное обучение не проводится, нормативные требования отсутствуют.

6. Лицензия или другой документ, дающий право на сферу «проектирование, монтаж, внедрение, обслуживание технических средств охраны» в Украине вообще не нужен.

7. Подготовка инженерно - технического персонала пультов охраны (вне зависимости от величины и принадлежности предприятия) оставляет желать лучшего. Насколько нам известно, профессиональное обучением не ведет ни одно из учебных заведений страны. В лучшем случае все ограничивается старым багажом знаний из ГСО, семинарами – обучением от производителя-поставщика и самообучением (благо есть Интернет).

8. Очень много объектовых средств сигнализации (ППК), которые установлены 5-ть и более лет назад и работают, используя устаревшие сегодня технологии (голосовой канал GSM, SMS, радио канал), без элементов имитостойкости.

9. Клиент, пульты охраны должны понимать, что, покупая сегодня оборудование (сигнализацию), он покупает технологию сегодняшнего дня. И если завтра тот же оператор связи предоставит более современные каналы связи (3G 4G 4G+) с новыми возможностями, то оборудование, что установлено на объекте сегодня в недалеком будущем уже не будет современным, а потом вообще уйдет из режима обслуживания.

10. На момент проверки нам не удалось найти ни одного оборудования (Приемо – Контрольные Приборы, датчики и сопутствующее оборудование) со степенью безопасности выше 2-го класса. А это означает, что почти все объекты на территории Украины оборудованы средствами охранной сигнализации, которые могут противостоять злоумышленникам, которые «будут иметь ограниченное знание систем охранной сигнализации и будут использовать обычный диапазон инструментальных средств и портативных инструментов», а от злоумышленников, которые «будут ознакомлены с системами охранной сигнализации» оборудования нет!!!

11. Предприятия охраны, которые оказывают Лицензионную услугу по охране объектов техническими средствами, в большинстве своем вообще не обращают внимание на условия Сертификата и пункты соответствия «ДСТУ» и на сегодняшний день, оборудуя объекты техническими средствами охраны отечественного производства, автоматически классифицируют их 2-ым классом степени безопасности, будь то киоск по продаже мясной продукции или банковское учреждение.

12. И, на наш взгляд, самое главное – заложником этого всего является Клиент, который, являясь в большинстве своем не профессионалом в вопросах безопасности, целиком полагается на «специалиста – профессионала», который приходит к нему с пульта охраны.

Данная информация предназначена.

- Прежде всего для Клиентов, которые должны задать вопрос своему охранному предприятию, что оно сделало для обеспечения надежности охраны (имитостойкость, оснащенность и пр.) его объекта, какое оборудование применило.

ОБЩЕСТВЕННАЯ ОРГАНИЗАЦИЯ «ВСЕУКРАИНСКОЕ ОБЪЕДИНЕНИЕ СПЕЦИАЛИСТОВ БЕЗОПАСНОСТИ» _____ **ЛОЩИЛИН О.Ю.**

- Для страховых компаний, которые в своих договорах страхования имущества определяют степень риска и в соответствии с ним страховой тариф.

- Для общественных объединений, союзов, организаций, предприятий, которые разрабатывают, согласовывают, устанавливают правила (положения, задания и пр.) по обеспечению безопасности с использованием технических систем.

- Для руководителей и собственников охранных предприятий, которые в основной массе доверяют техническую политику своих предприятий наемным техническим специалистам.

Хотим отметить, что это первая часть аналитической информации по теме «Крипто и имито стойкость охранного оборудования и систем». В других частях мы планируем рассмотреть вопросы – детального анализа анонсированных и рекомендованных производителем мероприятий, изучить тему «закрытых VPN-сетей предоставляемых оператором мобильной связи», более глубоко изучить тему Сертификации охранного оборудования с учетом принятых Национальных стандартов.

Помимо указанных в тексте руководителей и специалистов предприятий производителей и поставщиков, в подготовке данного документа принимали участие руководители и технические специалисты многих предприятий охраны, а именно: ***Руководитель предприятия охраны Гордеев А. Е, Главный специалист предприятия охраны Охрименко А.В., Главный специалист предприятия охраны Дзюба Н.В., Инженер пульта охраны Скорупский А.С., Технический руководитель предприятия охраны Клепов А.А., Начальник пульта охраны Цибарт А.В., Начальник пульта охраны Федюкин В.В., Руководитель предприятия охраны Карась С.В., Инженер пульта охраны Гуска О.В., Начальник пульта охраны Зайцев А.А., Инженер пульта охраны Бек А.О., Директор предприятия охраны Петришин Р.П., Инженер пульта охраны Божейкин В.Г.***

Глава правления **Лощилин О.Ю.**