

УДК 004.056

Имитозащита беспроводных автоматизированных систем охраны режимных объектов

Орлов А. В., Мельников Е. В., Финько О. А.

Постановка задачи. Высокую популярность для охраны режимных объектов (РО) различного назначения, особенно мобильного типа, с жёсткими требованиями к скорости приведения их в необходимое состояние готовности, получили беспроводные автоматизированные системы охраны (АСО), основанные на использовании радиосетей с ячеистой топологией (т.н. mesh-сетей, беспроводных сенсорных сетей и пр.). Основным преимуществом таких систем охраны является высокая скорость развертывания/сворачивания, что особенно важно для охраны объектов мобильного типа. Другое важное преимущество АСО – простота масштабируемости при охране объектов различной площади и конфигурации, а также при их модернизации. Функционирование данных систем на основе использования радиоканала для передачи служебных сообщений актуализирует вопросы обеспечения безопасности передаваемых данных от имитационных воздействий потенциального злоумышленника. Использование известного способа обеспечения имитозащиты данных, основанного на выработке имитовставки, может привести к возрастанию вероятности компрометации ключевой информации при увеличении количества охранных извещателей и, следовательно, выходу АСО из состояния необходимого уровня защищенности. **Целью статьи** является повышение уровня имитозащищенности данных, передаваемых по радиоканалам АСО РО. Предложены алгоритмы защиты данных от имитационных воздействий злоумышленника на различных этапах функционирования системы охраны, а также методика обеспечения имитозащиты данных, особенности построения и функционирования АСО РО в защищенном режиме. **Используются методы:** теории алгоритмов и формализованного описания криптографических протоколов; элементы теории случайных процессов (при оценивании защищенности системы охраны). **Новизна** предложенных алгоритмов и методики заключается в новых правилах и приёмах комплексирования известных криптографических алгоритмов и протоколов, а также различных их режимов функционирования, обеспечивающих защиту радиоканалов АСО РО от различных типов имитационных воздействий злоумышленника. **Результаты:** комплекс алгоритмов защиты данных, передаваемых между элементами системы охраны, от имитационных воздействий злоумышленника, позволяющий осуществлять контроль данных на каждом из этапов их прохождения между элементами системы; методика обеспечения имитозащиты данных, включающая в себя ряд научно-технических предложений, направленных на обеспечение защищенности данных от имитационных воздействий злоумышленника. Выполнено оценивание защищенности системы охраны. **Практическая значимость.** Полученные результаты позволяют создавать АСО РО, имеющие возможность безопасного функционирования в условиях имитационных воздействий злоумышленника на нее. При этом предлагаемые протоколы основаны на существующих и стандартизированных в Российской Федерации криптографических алгоритмах.

Ключевые слова: автоматизированная система охраны, беспроводные сенсорные сети, имитовставка, имитозащита данных, имитоустойчивость радиоканала, криптографические алгоритмы и протоколы, охрана режимных объектов, хеш-функция, электронная подпись, mesh-сети.

Библиографическая ссылка на статью:

Орлов А. В., Мельников Е. В., Финько О. А. Имитозащита беспроводных автоматизированных систем охраны режимных объектов // Системы управления, связи и безопасности. 2020. № 3. С. 22-64. DOI: 10.24411/2410-9916-2020-10302.

Reference for citation:

Orlov A. V., Melnikov E. V., Finko O. A. Imitation Protection of Wireless Automated Security Systems for Sensitive Objects. Systems of Control, Communication and Security, 2020, no. 3, pp. 22-64. DOI: 10.24411/2410-9916-2020-10302 (in Russian).

Актуальность

Автоматизированные системы охраны (АСО) являются одной из ключевых составляющих системы физической защиты важных государственных и военных объектов и предназначены для надёжного обнаружения несанкционированного доступа на объекты охраны и управления техническими средствами охраны [1, 2].

К числу важнейших объектов охраны следует отнести, прежде всего, режимные объекты (РО), под которыми в соответствии с Указом Президента [3] следует понимать военные и специальные объекты, воинские части, предприятия, организации, учреждения, для функционирования которых установлены дополнительные меры безопасности.

Одной из важнейших характеристик систем охраны следует считать устойчивость их функционирования в условиях воздействия различных деструктивных факторов.

Цикл действия мобильных РО включает четыре основных этапа (не считая техническое обслуживание, ремонт, консервацию и пр.): перемещение, развертывание, функционирование на позиции, свёртывание.

Наиболее уязвимы РО на этапах развертывания и свёртывания. Чем короче эти этапы – тем выше уровень защищённости РО (ниже вероятность деструктивного воздействия, компрометации конфиденциальной информации и пр.) при иных равных условиях. Следовательно, важно обеспечить снижение длительности указанных этапов.

Обеспечить высокую оперативность развертывания и свёртывания РО позволяют беспроводные АСО РО, которые могут быть исполнены как на основе только радиолиний связи (удалённые подступы объекту), так и по гибридной технологии – совместно с использованием других (проводных, оптоволоконных) физических линий связи.

Примером таких систем могут служить принятые на снабжение рядом силовых ведомств Российской Федерации комплексы: «Радий-БРК», «Стрелец-часовой-2» (на основе распределённых микросотовых сетей), «Радиобарьер» и др. [1]. Наиболее перспективным вариантом структуры беспроводных АСО РО является построение их на основе радиосетей с ячеистой топологией (mesh-сетей) [4–6].

Распределённые ячеистые сети обладают рядом преимуществ, прежде всего – простотой масштабирования сети для объектов охраны различной площади и различной конфигурации. При этом характеристики радиоканала в таких сетях остаются приблизительно постоянными, радиосредства извещателей – идентичными. Низкая мощность радиопередатчика – порядка долей или единиц мВт – обеспечивает высокую продолжительность автономного функционирования извещателей и хорошую разведзащищённость.

К недостаткам таких АСО, как и любых других АСО, выполненных на основе радиосетей, относится высокая подверженность внешним деструктивным воздействиям, которые могут полностью блокировать работу системы охраны. Таким образом, основным уязвимым элементом беспроводных АСО РО является радиоканал и радиосеть в целом [7].

Краткий анализ факторов деструктивного воздействия на беспроводные АСО РО

Принцип построения беспроводной АСО РО, основанной на использовании технологии ячеистых распределённых сетей, поясняется с помощью рис. 1.

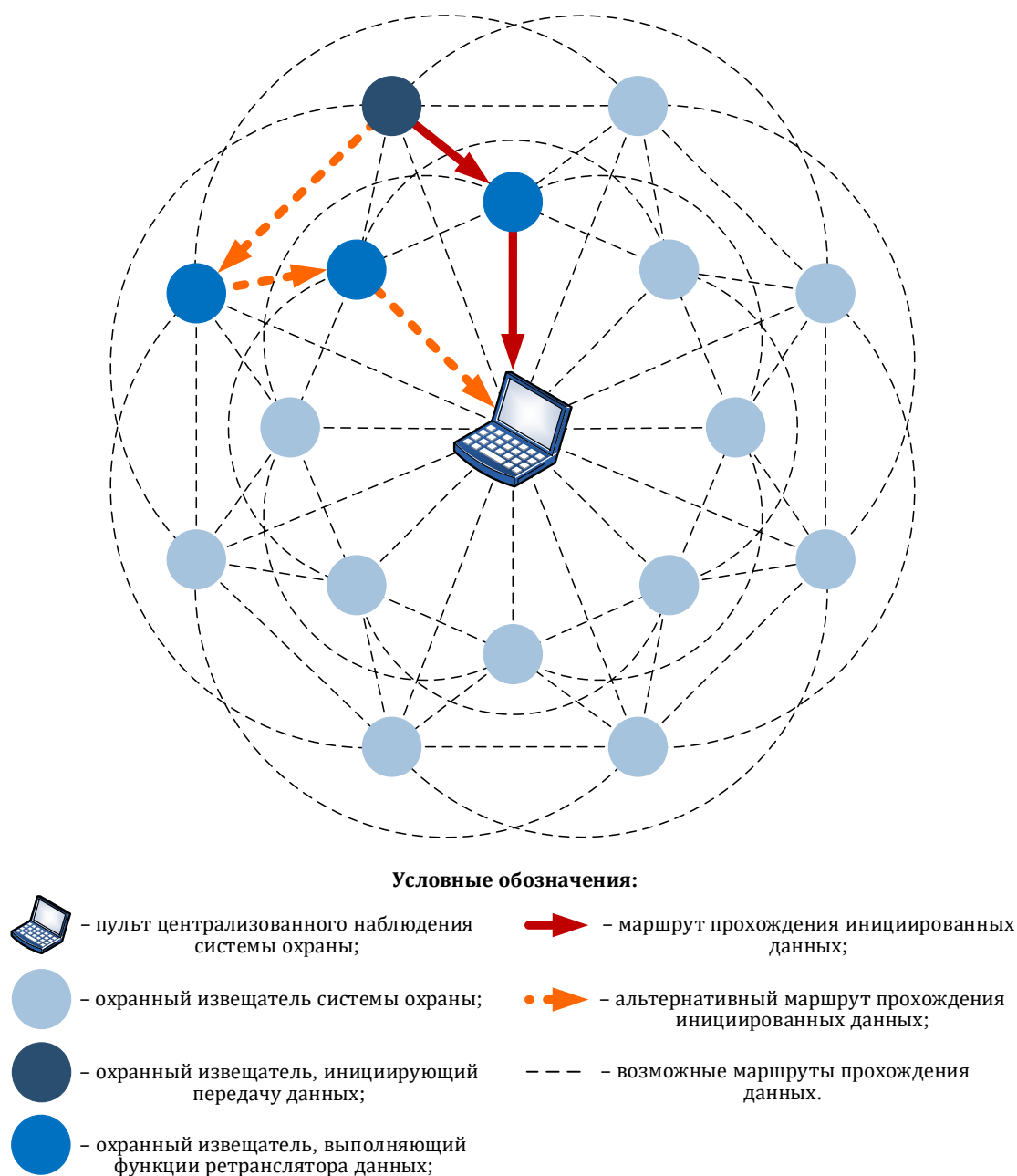


Рис. 1. Схематическое пояснение построения АСО РО

В отечественной [8–15] и зарубежной литературе [16–25] опубликован ряд работ, посвящённых исследованию различных аспектов защиты радиоканалов и беспроводных сенсорных сетей от деструктивных воздействий.

Далее будем различать понятия *физической безопасности* объектов охраны и *безопасности информации*, циркулирующей в АСО РО, обеспечивающей процесс её надёжного функционирования при различных деструктивных воздействиях на информацию.

Физическая безопасность (ФБ) – состояние физической защищенности жизненно важных интересов и ресурсов объекта охраны от угроз, источниками которых являются противоправные (несанкционированные) действия физических лиц (нарушителей) или от преступных посягательств физических лиц (нарушителей) [26].

Безопасность информации (БИ) – состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность [27].

Угрозы ФБ и БИ. Будем различать понятия «угроза ФБ» и «угроза БИ». Также будем считать, что реализация угрозы БИ в АСО РО всегда направлена на реализацию угрозы ФБ РО (рис. 2).

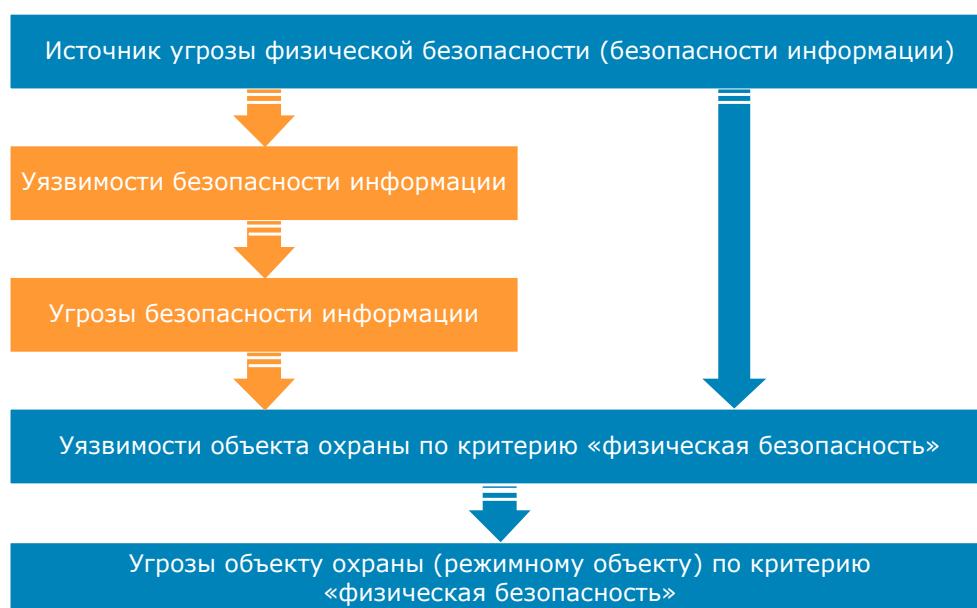


Рис. 2. Характеристика причинно-следственной взаимосвязи уязвимостей и угроз АСО РО по критерию физической безопасности и по критерию безопасности информации

К основным факторам (физическим и информационным) воздействия на беспроводные АСО РО, приводящим к реализации угроз БИ, а затем и ФБ, можно отнести (рис. 3):

1) огневое поражение с помощью огневых и ударных средств, механическое разрушение с помощью роботов, применение ослепляющих (в радиоволновом, оптическом, инфракрасном и др. диапазонах волн) аэрозолей, образуемых ими покрытий и пр.;

2) энергетическое подавление, в том числе с использованием оружия, основанного на новых физических принципах (ЭМИ и пр.);

3) имитационное «подавление» – наиболее эффективное, так как требует минимальных затрат злоумышленника.



Рис. 3. Виды и способы деструктивных воздействий на АСО РО и характеристика их последствий

Рассмотрим варианты исполнения беспроводных АСО РО, основные уязвимости безопасности информации (БИ) и варианты их устранения.

Ограничение. Рассматриваются АСО РО без привязки к конкретному объекту охраны, без учёта параметров площади объекта, глубины рубежей охраны, параметров радиосредств, используемых в охранных извещателях; охранные извещатели по возможностям радиосвязи считаются идентичными.

Вариант 1 построения сети (В 1). АСО РО базируется на основе распределённой системы с ячеистой топологией. Защита данных, передаваемых на канальном и более высоких уровнях модели OSI от умышленных деструктивных воздействий, отсутствует.

Защита таких сетей должна строиться на физическом уровне модели OSI: обеспечение скрытности передачи извещений за счёт понижения мощности радиоизлучения, применения специальных видов модуляции радиосигнала, расширения полосы частот передаваемого сигнала различными методами [32], применения пространственно ориентированных антенных систем, в частности управляемых фазированных антенных решёток и пр.

Сценарий 1. Злоумышленник подавляет радиосеть АСО РО с помощью генерации радиосигнала в заданной полосе частот с более высоким, чем уровень радиосигнала в сети, энергетическим уровнем.

В этом случае нормальное функционирование сети невозможно, возникает состояние реализации угрозы БИ – «отказ в обслуживании». Как следствие, это должно приводить к реализации потенциальной возможности несанкционированного доступа злоумышленника на охраняемый объект. Однако в данной работе будем использовать следующее допущение.

Допущение 1. АСО РО оснащена средствами и алгоритмами, способными идентифицировать факт энергетического подавления радиосети (обнаружение подавляющей радиопомехи, обнаружение факта прекращения обмена охранных извещателей с пультом централизованного наблюдения (ПЦН) служебными сообщениями и пр.).

В этом случае оператор АСО РО переводит систему в другой режим функционирования: выставление постов, патрулей, «секретов» и пр. Уязвимостью АСО РО будет являться возможность использования злоумышленником интервала времени, в течение которого он способен проникнуть на охраняемый

объект и нанести ущерб. Устранение такой уязвимости достигается соответствующим проектированием и размещением средств физической защиты охраняемого объекта, обеспечивающих задержку продвижения нарушителя, достаточную для успешного реагирования группы физического противодействия.

Таким образом, в соответствии с принятым допущением 1, при реализации сценария 1 злоумышленник не имеет возможности реализовать угрозу БИ *«отказ в обслуживании»*.

Сценарий 2. Злоумышленник способен преодолеть защиту физического уровня модели OSI [28] и генерировать охранные извещения со структурой идентичной, используемой в сети АСО РО.

Тогда злоумышленник способен блокировать нормальную работу АСО РО путём массовой генерации ложных срабатываний, то есть реализовать угрозу БИ *«отказ в обслуживании»*. Распознать такую атаку не сложно, и оператор АСО РО аналогично действиям в соответствии со сценарием 1, должен перевести АСО РО в режим функционирования, обеспечивающий состояние физической защищённости объекта охраны.

При этом сценарии злоумышленник может ставить и другую цель: истощение заряда батарей.

Уязвимость 1. Злоумышленник способен имитировать охранные извещения о нормальном функционировании извещателей, сигналов об отсутствии тревоги, а также имитировать единичные сигналы тревоги отвлекающего характера. В этом случае злоумышленник способен осуществить атаку БИ *«отказ в обслуживании»* [29] – наиболее опасную, ввиду скрытности её реализации от оператора АСО РО.

Таким образом, наивысшая опасность имитационных атак злоумышленника состоит в его способности реализации угрозы БИ *«отказ в обслуживании»* путем инициализации скрытых состояний «ошибки 1-го или 2-го рода». Тогда злоумышленник имеет все шансы успешного проникновения на охраняемый объект.

Для предотвращения реализации угрозы *«отказ в обслуживании»* требуется построение распределённых радиосетей со встроенными средствами защиты от имитации злоумышленника на канальном и более высоких уровнях модели OSI.

Вариант 2 построения сети (В 2). Сеть строится в соответствии с вариантом 1 и в неё дополнительно встраиваются криптографические средства защиты сигналов извещений от имитации в соответствии с одним из криптографических протоколов [30]. В этом случае все охранные извещатели снабжаются единым (для всей сети) секретным ключом, необходимым для формирования имитовставки или ключевой хеш-функции. Единственное преимущество такого способа построения ключевой системы – простота в построении сети и обслуживании, так как все извещатели – одинаковые (для замены охранного извещателя не требуется предварительной записи в него индивидуального ключа и записи нового ключа в ПЦН).

Любые попытки злоумышленника действовать в соответствии с первым или вторым сценарием будут обнаружены.

Допущение 2. Для защиты радиоканалов сети от имитации используются алгоритмы, определённые актуальными криптографическими стандартами. Поэтому будем считать, что вероятность успешного анализа используемого шифра (вскрытия ключа) ничтожно мала.

Сценарий 3. Злоумышленник овладевает секретным ключом, то есть компрометирует его.

Допущение 3. Любые попытки злоумышленника завладеть секретным криптографическим ключом (кража охранного извещателя, попытка вскрыть его и пр.) успешно обнаруживаются (регулярный обмен в сети извещениями об исправности извещателей, физическая защита ключа с помощью изготовления специальных микросхем, стирание ключа при попытке вскрытия извещателя, снижении заряда батарей ниже допустимого уровня, изменение пространственного положения охранного извещателя и пр.).

Опасность этой ситуации заключается в том, что для компрометации всей сети злоумышленнику достаточно завладеть только одним ключом (так как все используемые ключи – одинаковые).

$$P_{\text{компрмет. сети}} \approx P_{\text{компр. извещателя}}, \quad (1)$$

где $P_{\text{компрмет. сети}}$ – вероятность компрометации охранной сети, $P_{\text{компр. извещателя}}$ – вероятность компрометации охранного извещателя (ключа) (знак «приблизительно равно» использован в связи с тем, что, строго говоря, компрометация может быть одного и более одинаковых ключей).

В этих условиях при компрометации ключа оператор лишён возможности оперативной (дистанционной) замены ключей – для каждого извещателя должна быть выполнена процедура замены ключа.

Уязвимость 2. При компрометации одного извещателя в сети будет утрачен необходимый уровень защищённости *на длительное время*.

Уязвимость 3. Как и при сценарии 2 злоумышленник может ставить целью истощение заряда батарей и, как следствие, их замену со снижением необходимого уровня защищённости сети на длительное время.

Сценарий 4. Злоумышленник осуществляет запись и повтор ранее переданной сигнальной информации с известными параметрами работы извещателей.

Для противодействия такого рода атаке применяется так называемая «метка времени». В течение заданного интервала времени метка устаревает и при приёме сигнала с такой меткой он признаётся нелегитимным.

Вариант 3 построения сети (В 3). Все охранные извещатели сети снабжаются индивидуальными секретными ключами, необходимыми для выработки имитовставок от отправляемых извещений. Уровень защищённости такой сети будет значительно выше, чем в случае её построения в соответствии с вариантом 2.

Сценарий 5. Злоумышленник компрометирует (что обнаруживается в соответствии с допущением 3) один или несколько криптографических ключей.

Для успешной реализации обнаруживаемой атаки «отказ в обслуживании» злоумышленнику необходимо скомпрометировать не менее, чем по одно-

му извещателю из каждого рубежа охраны, что довольно затруднительно, и, следовательно, менее вероятно.

Таким образом, значение вероятности компрометации охранной сети можно вычислить по формуле:

$$P_{\text{компр. сети}} = \prod_{i=1}^j \left(1 - \left(1 - P_{\text{компр. извещателя}} \right)^{n_i} \right), \quad (2)$$

где $P_{\text{компр. сети}}$ – вероятность компрометации охранной сети, $P_{\text{компр. извещателя}}$ – вероятность компрометации охранного извещателя (ключа), j – количество рубежей охраны системы, n_i – количество охранных извещателей в i -м рубеже охраны.

При этом контактной замене подлежат ключи только скомпрометированных извещателей. Время, требуемое на выполнение этой операции, существенно меньше, по сравнению с вариантом 2 построения сети.

Сценарий 6. Злоумышленник осуществляет ретрансляцию радиосигнала в реальном времени (с актуальной «меткой времени»), вырабатываемого извещателем, установленным в заданном участке территории, в извещатель, установленный в другом участке. Он может ретранслировать сигналы с параметрами «норма» или «тревога» (путем, например, использования роботов), имитируя тем самым отвлекающие действия. Уязвимость 3 остаётся актуальной.

Уязвимость 4. Злоумышленник реализует угрозы БИ «отказ в обслуживании» путем создания скрытых состояний «ошибки 1, 2-го рода».

Уязвимость 5. Кратковременная реализация угрозы БИ «отказ в обслуживании» путём вызова перегрузки отдельных участков сети с помощью имитации ложных извещений (например, ошибок 2-го рода). При этом легитимный сигнал тревоги может быть заблокирован вызванным отказом. С учётом возможностей современных средств обработки информации данный вид атаки может быть реализован синхронно с продвижением нарушителя к объекту охраны. Здесь «слабость» и ограниченный объем ресурсов используемых сетевых технологий вызваны необходимостью ограничения потребления энергоресурсов батарей и стоимостью извещателей.

Допущение 4. Если объект охраны – объект информатизации на котором может обрабатываться конфиденциальная информация, токопроводящие тракты объекта информатизации располагаются на безопасном (в соответствии с нормативными документами) удалении от токопроводящих трактов АСО РО (при необходимости могут быть использованы любые другие пассивные, а также активные средства технической защиты информации).

В связи с данным допущением, у объекта информатизации, на котором может обрабатываться конфиденциальная информация, уязвимости, связанные с возможностью утечки конфиденциальной информации по техническим каналам посредством АСО РО, *отсутствуют*.

Способ защиты радиосети АСО РО от имитационных воздействий злоумышленника (В 4)

Несмотря на определённые преимущества, недостатками варианта 3 построения сети (В 3) является сохранение уязвимостей 3–5, преимущественно связанных с возможностью беспрепятственного распространения и размножения нелегитимных (имитированных) сигналов по сети.

В основу предлагаемого решения положим принцип разбиения всей сети с множеством охранных извещателей $\{a_i | i = \overline{1, N}\}$, где a_i – условный номер i -го охранного извещателя, N – общее количество извещателей, на множество $\{z_i | i = \overline{1, t}\}$ пересекающихся локальных участков – зон, образованных исходя из предельных, для требуемого уровня устойчивости функционирования сети, параметров физического взаимодействия радиосредств охранных извещателей, где z_i – условный номер i -й зоны, включающей в себя охранные извещатели АСО РО, t – общее количество зон (рис. 4). Пересечение зон необходимо для обеспечения контроля охранными извещателями друг друга.

Кроме того, необходимые свойства сети получим комбинированным применением криптографических алгоритмов выработки имитовставки и вычисления электронной подписи (включая хеш-функцию).

В каждом i -м охранном извещателе записываются:

- 1) индивидуальный секретный ключ k_i выработки имитовставки;
- 2) индивидуальный ключ d_i подписи;

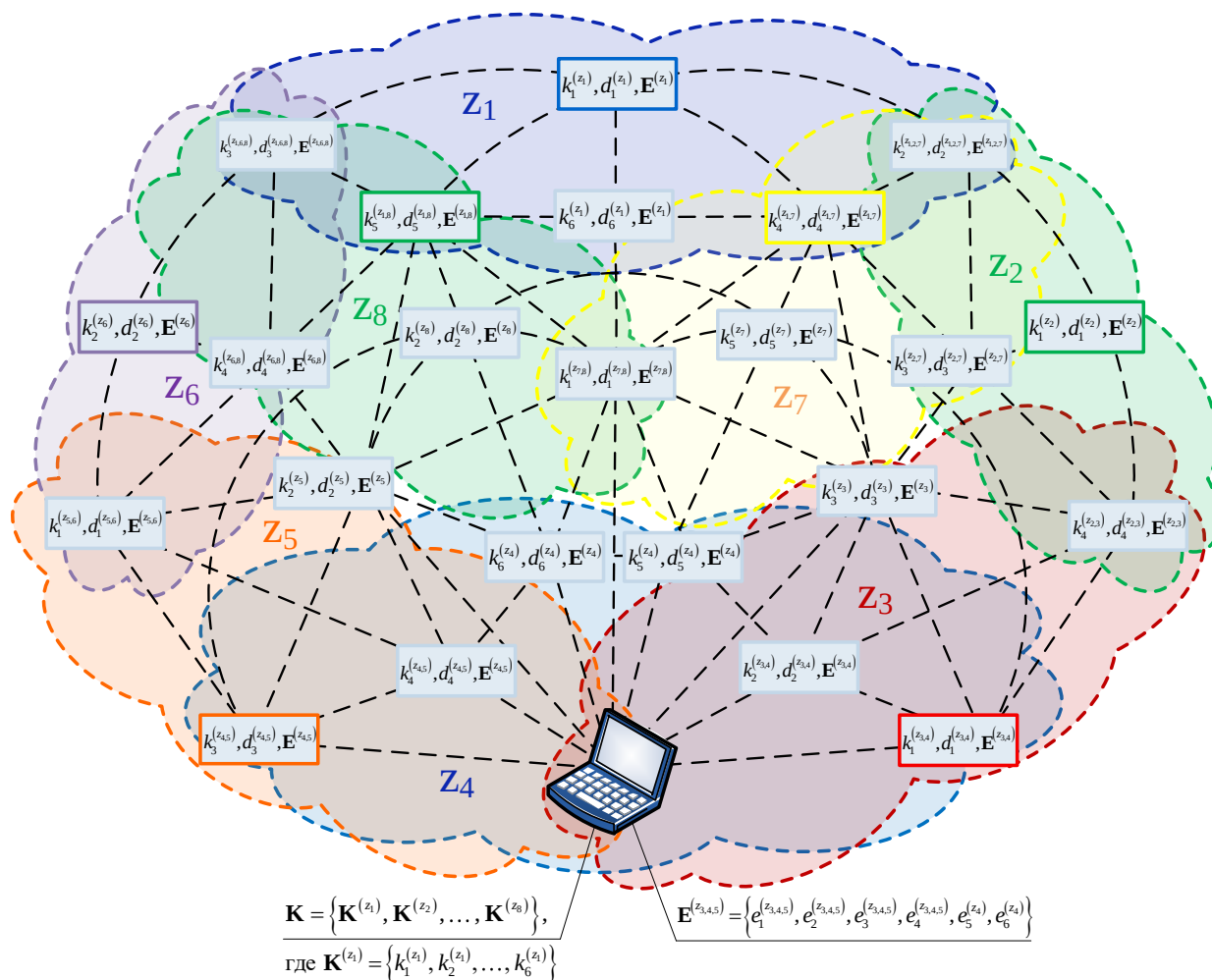
3) база (массив) ключей $E^{(z_i)} = \{e_p | p = \overline{1, O}\}$, где z_i – номер зоны для конкретного охранного извещателя, e_p – ключи проверки подписи, тех охранных извещателей, которые находятся в пределах физической досягаемости передачи извещений друг другу, O – общее количество извещателей, находящихся в пределах физической досягаемости передачи извещений.

В ПЦН размещаются ключи:

1) массив всех индивидуальных секретных ключей $\{k_i | i = \overline{1, N}\}$ выработки имитовставки;

2) база (массив) ключей $\{e_i | i = \overline{1, H}\}$ проверки подписи, тех охранных извещателей, которые находятся в пределах физической досягаемости передачи извещений на ПЦН, где H – общее количество извещателей, находящихся в пределах физической досягаемости передачи извещений.

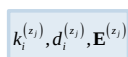
Таким образом, в сети реализуется принцип взаимодействия параметров физического и канального (в части, касающейся защиты информации) уровней модели OSI.



Условные обозначения:



– пульт централизованного наблюдения системы охраны



– охранной извещатель системы охраны



– возможные маршруты прохождения данных



– зоны физической досягаемости радиоканалов связи между извещателями

Рис. 4. Пояснение принципа построения радиосети АСО РО с фрагментацией охранных извещателей и размещённых в них криптографических ключей

В соответствии с рассмотренным решением, разработаем комплекс алгоритмов имитозащиты данных, передаваемых по радиоканалам АСО РО.

Алгоритм формирования данных в охранном извещателе. В качестве исходных данных для вычисления имитовставки используется массив $\{B_p \mid p = \overline{1, l}\}$ векторных данных, подлежащих передаче по сети АСО РО. В качестве аргумента функции ЭП используется результат операции конкатенации массива данных и значения имитовставки.

Блок-схема алгоритма представлена на рис. 5.

Ввод:

$\{\mathbf{B}_p \mid p = \overline{1, l}\}$ – массив данных, подлежащих передаче по радиоканалу АСО РО, где l – длина массива; k_j – ключ вычисления имитовставки; d_j – ключ ЭП.

Шаг 1:

Вычислить значение имитовставки $\mathbf{I}_p$ от вектора данных $\mathbf{B}_p$, подлежащих передаче по радиоканалу для $p = \overline{1, l}$:

$$\begin{cases} \mathbf{I}_1 = E_{\text{им}}(k_j, \mathbf{B}_1); \\ \mathbf{I}_2 = E_{\text{им}}(k_j, \mathbf{B}_2); \\ \dots\dots\dots; \\ \mathbf{I}_l = E_{\text{им}}(k_j, \mathbf{B}_l). \end{cases}$$

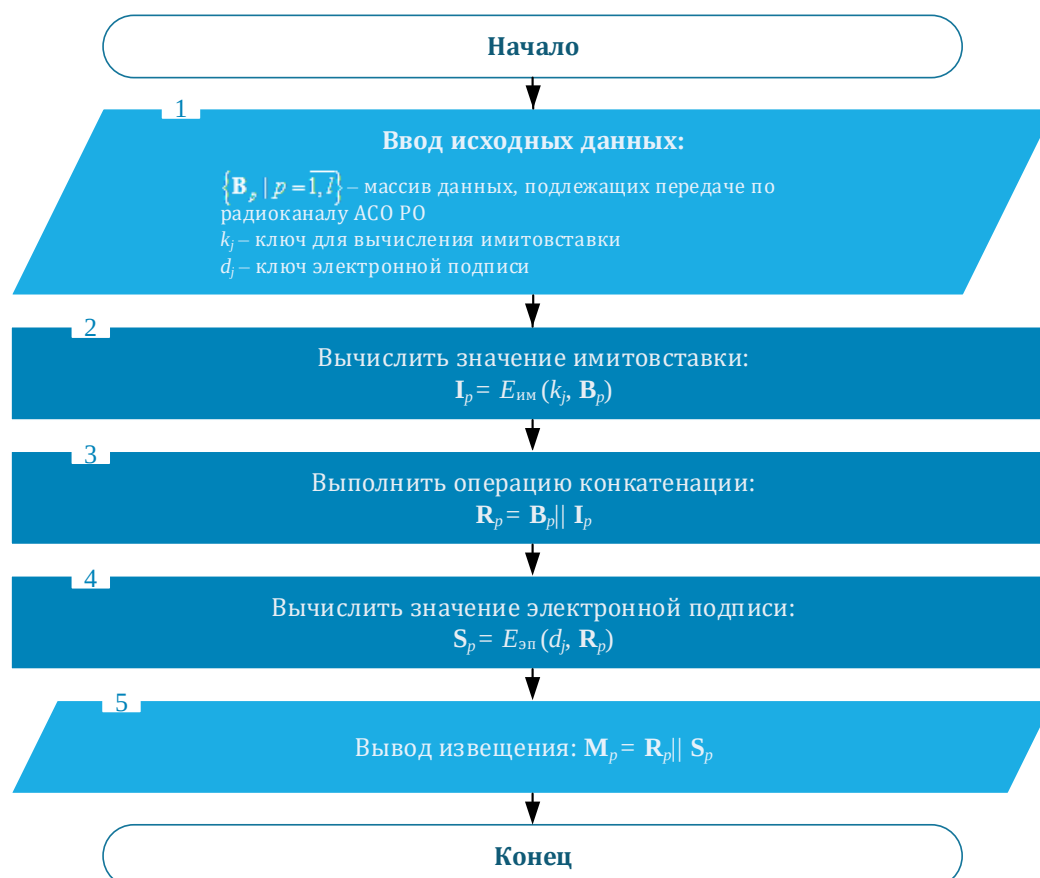


Рис. 5. Блок-схема алгоритма формирования данных в охранном извещателе АСО РО

Шаг 2:

Выполнить конкатенацию:

$$\begin{cases} \mathbf{R}_1 = \mathbf{B}_1 \parallel \mathbf{I}_1; \\ \mathbf{R}_2 = \mathbf{B}_2 \parallel \mathbf{I}_2; \\ \dots\dots\dots; \\ \mathbf{R}_l = \mathbf{B}_l \parallel \mathbf{I}_l. \end{cases}$$

Шаг 3:

Вычислить значение $\mathbf{S}_p$ ЭП от данных $\mathbf{R}_p$ с использованием ключа подписи d_j , определенного охранному извещателю:

$$\begin{cases} \mathbf{S}_1 = E_{\text{эп}}(d_j, \mathbf{R}_1); \\ \mathbf{S}_2 = E_{\text{эп}}(d_j, \mathbf{R}_2); \\ \dots\dots\dots; \\ \mathbf{S}_l = E_{\text{эп}}(d_j, \mathbf{R}_l). \end{cases}$$

Шаг 4:

Сформировать массив $\mathbf{M}_p$, подлежащий передаче на ПЦН:

$$\begin{cases} \mathbf{M}_1 = \mathbf{R}_1 \parallel \mathbf{S}_1; \\ \mathbf{M}_2 = \mathbf{R}_2 \parallel \mathbf{S}_2; \\ \dots\dots\dots; \\ \mathbf{M}_l = \mathbf{R}_l \parallel \mathbf{S}_l. \end{cases}$$

Вывод результата:

$$\begin{cases} \mathbf{M}_1 = \mathbf{B}_1 \parallel \mathbf{I}_1 \parallel \mathbf{S}_1; \\ \mathbf{M}_2 = \mathbf{B}_2 \parallel \mathbf{I}_2 \parallel \mathbf{S}_2; \\ \dots\dots\dots; \\ \mathbf{M}_l = \mathbf{B}_l \parallel \mathbf{I}_l \parallel \mathbf{S}_l. \end{cases}$$

Алгоритм функционирования охранного извещателя-ретранслятора.

В охранном извещателе осуществляется хранение ключа k_g для вычисления имитовставки, ключа подписи d_g для вычисления ЭП, а также базы данных ключей проверки подписи $\mathbf{E}_g$ для проверки ЭП данных, поступивших на охранный извещатель.

Блок-схема алгоритма представлена на рис. 6.

Ввод:

$\{\mathbf{M}_p = (\mathbf{R}_p \parallel \mathbf{S}_p) \mid p = \overline{1, l}\}$ – массив данных, поступивших на охранный извещатель, выполняющий функции ретранслятора, где $\mathbf{R}_p = \mathbf{B}_p \parallel \mathbf{I}_p$; $\mathbf{S}_p$ – значение

ЭП, вычисленное от $\mathbf{R}_p$; d_g – ключ подписи для вычисления ЭП; e_j – ключ проверки подписи, где $e_j \in \mathbf{E}_g$.

Шаг 1:

Выполнить проверку ЭП S_p^* от данных $\mathbf{R}_p$ с использованием ключа проверки e_j :

$$\begin{cases} S_1^* = D_{\text{эп}}(e_j, \mathbf{R}_1); \\ S_2^* = D_{\text{эп}}(e_j, \mathbf{R}_2); \\ \dots\dots\dots; \\ S_l^* = D_{\text{эп}}(e_j, \mathbf{R}_l). \end{cases}$$

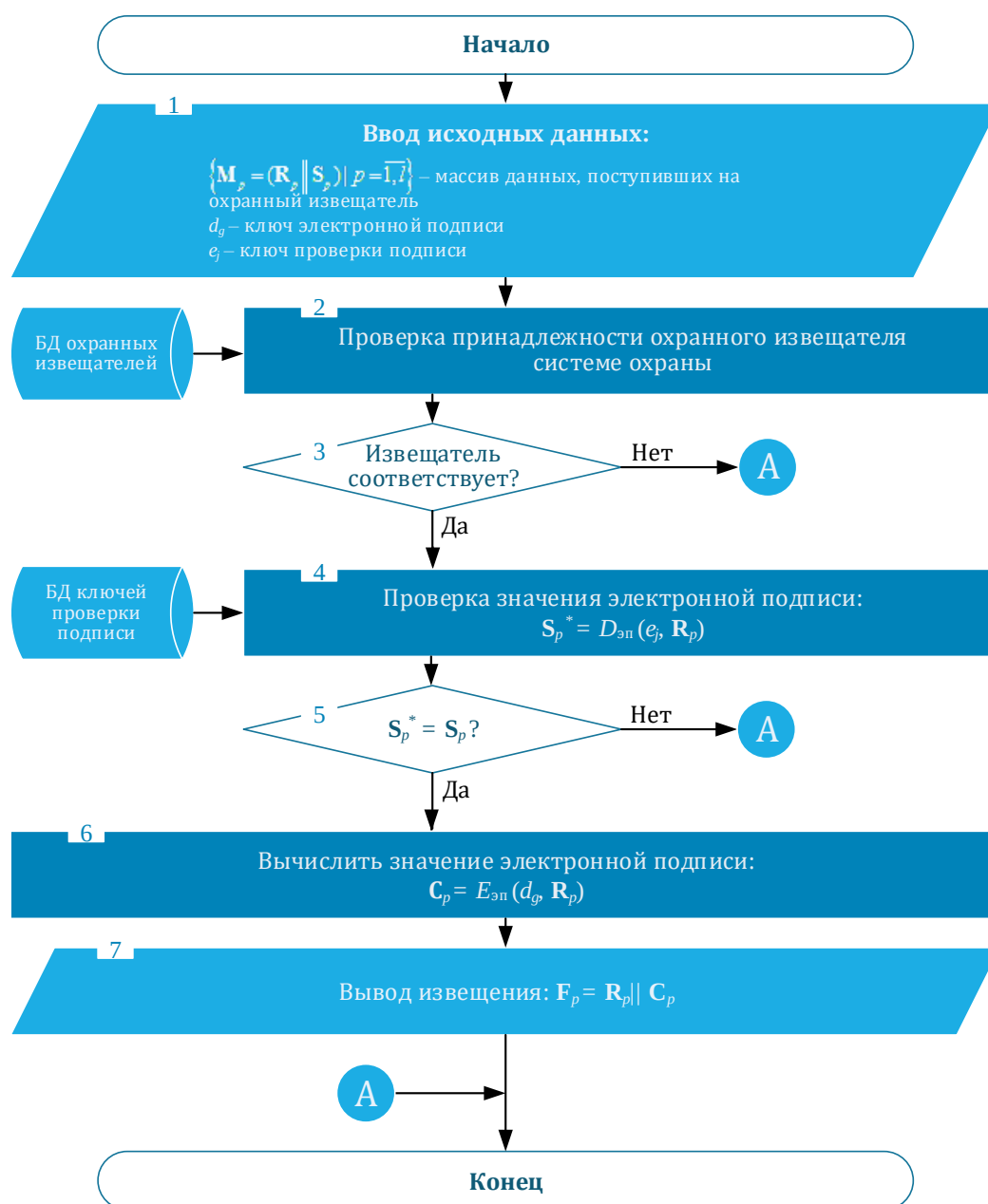


Рис. 6. Блок-схема алгоритма функционирования системы имитозащиты данных охранного извещателя, выполняющего функцию ретранслятора данных

Шаг 2:

Выполнить сравнение полученного значения S_p^* ЭП и поступившего с данными R_p значения S_p .

Если $S_p^* \neq S_p$, то делается вывод о нарушении подлинности поступивших данных R_p и возможном воздействии нарушителя. Охранным извещателем может (определяется оператором) формироваться служебное сообщение «Тревога», а данные R_p далее не передаются.

Если $S_p^* = S_p$, то принимается решение на дальнейшую обработку поступивших данных R_p .

Шаг 3:

Вычислить значение C_p ЭП от проверенных данных R_p с использованием ключа подписи d_g , определенного данному охранным извещателю:

$$\begin{cases} C_1 = E_{\text{эп}}(d_g, R_1); \\ C_2 = E_{\text{эп}}(d_g, R_2); \\ \dots\dots\dots; \\ C_l = E_{\text{эп}}(d_g, R_l). \end{cases}$$

Шаг 4:

Сформировать массив F_p , подлежащий передаче на ПЦН:

$$\begin{cases} F_1 = R_1 \parallel C_1; \\ F_2 = R_2 \parallel C_2; \\ \dots\dots\dots; \\ F_l = R_l \parallel C_l. \end{cases}$$

Вывод результата:

$$\begin{cases} F_1 = B_1 \parallel I_1 \parallel C_1; \\ F_2 = B_2 \parallel I_2 \parallel C_2; \\ \dots\dots\dots; \\ F_l = B_l \parallel I_l \parallel C_l. \end{cases}$$

Алгоритм имитозащиты данных в ПЦН. В ПЦН осуществляется хранение базы ключей $\{k_j \mid j = \overline{1, N}\}$ всех охранных извещателей функционирующих в системе, используемых для вычисления имитовставок, а также базы ключей $\{e_g \mid g = \overline{1, H}\}$ проверки подписей, тех охранных извещателей, которые находятся в пределах физической досягаемости.

Блок-схема алгоритма представлена на (рис. 7).

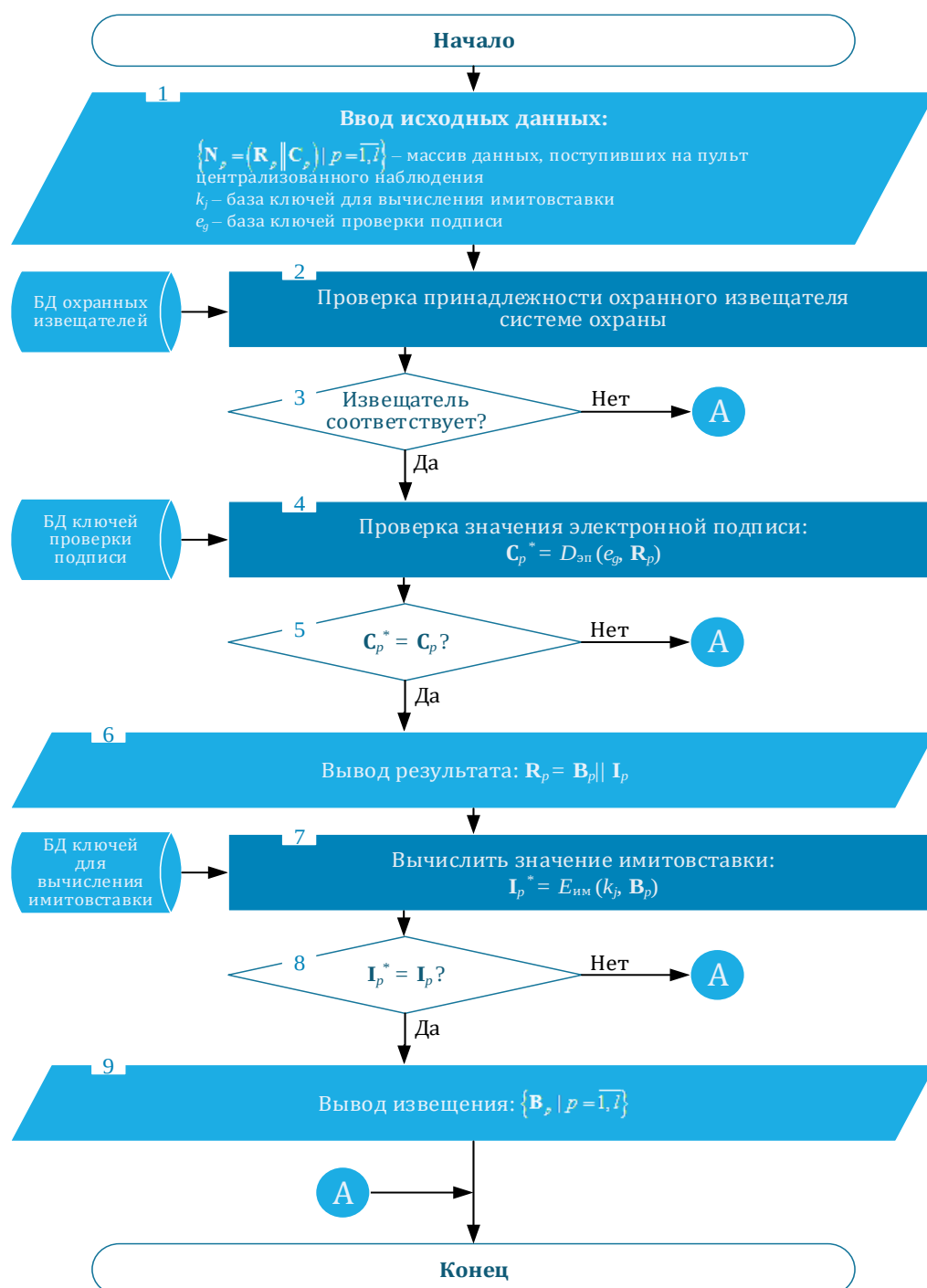


Рис. 7. Блок-схема алгоритма имитозащиты данных в ПЦН АСО РО

Ввод:

$\{N_p = (R_p || C_p) | p=1..l\}$ – массив данных, поступивших на ПЦН;

$R_p = B_p || I_p$; C_p – значение ЭП, вычисленное от данных R_p ; k_j – ключ для вычисления имитовставки; e_g – ключ проверки подписи.

Шаг 1:

Выполнить проверку значения C_p^* ЭП от поступивших данных R_p с использованием ключа проверки подписи e_g :

$$\begin{cases} C_1^* = D_{\text{эп}}(e_g, R_1); \\ C_2^* = D_{\text{эп}}(e_g, R_2); \\ \dots\dots\dots; \\ C_l^* = D_{\text{эп}}(e_g, R_l). \end{cases}$$

Шаг 2:

Выполнить сравнение C_p^* и поступившего с данными R_p значения C_p .

Если $C_p^* \neq C_p$, то делается вывод о нарушении подлинности поступивших данных R_p и возможного воздействия злоумышленника на данные, передаваемые по сети.

Если $C_p^* = C_p$, то принимается решение на дальнейшую обработку поступивших данных R_p .

Шаг 3:

Вычислить значение имитовставки I_p^* от данных B_p , подлежащих передаче по радиоканалу:

$$\begin{cases} I_1^* = E_{\text{им}}(k_j, B_1); \\ I_2^* = E_{\text{им}}(k_j, B_2); \\ \dots\dots\dots; \\ I_l^* = E_{\text{им}}(k_j, B_l). \end{cases}$$

Шаг 4:

Выполнить сравнение вычисленного значения имитовставки I_p^* и поступившего с данными R_p значения I_p .

Если $I_p^* \neq I_p$, то делается вывод о нарушении целостности поступивших данных R_p и возможном воздействии злоумышленника.

Если $I_p^* = I_p$, то делается вывод об отсутствии нарушения целостности полученных данных и функционировании АСО РО в штатном режиме.

Таким образом, рассмотренный комплекс алгоритмов имитозащиты данных позволяет обеспечить защиту данных, циркулирующих между элементами АСО РО.

Методика обеспечения имитозащиты данных, передаваемых по радиоканалам АСО РО

Исследования в области безопасного функционирования АСО РО ведутся на протяжении многих лет и затрагивают различные ее стороны, например, принципы построения и развитие теории ее защиты, а также стандарты оценки ее надежности [1, 31]. Наиболее эффективно задачи защиты информации решаются в рамках упреждающей стратегии защиты, когда на этапе проектирова-

ния оцениваются потенциально возможные угрозы и реализуются механизмы защиты от них [32].

Предложенный выше комплекс алгоритмов имитозащиты данных, передаваемых по радиоканалам АСО РО, может использоваться в условиях применения дополнительных решений, обеспечивающих их необходимую эффективность.

Пространственная декомпозиция АСО РО. Функционирование АСО РО может быть организовано для охраны протяженных по площади территорий. При этом увеличивается количество охранных извещателей, что в свою очередь, оказывает влияние на безопасность функционирования системы охраны, а именно:

- возрастает вероятность компрометации ключей, хранящихся в охранных извещателях;
- увеличивается длительность обслуживания системы защиты информации – осуществления генерации и смены ключей в охранных извещателях;
- усложняются условия обслуживания элементов системы охраны (техническое обслуживание и ремонт элементов системы).

Для организации функционирования АСО РО в защищенном режиме при условии необходимости организации охраны протяженных по площади РО рассмотрим способ пространственной декомпозиции системы разнесенных, а также пересекающихся охраняемых периметров РО с иерархическим и центральным одноуровневым управлением (рис. 8, 9).

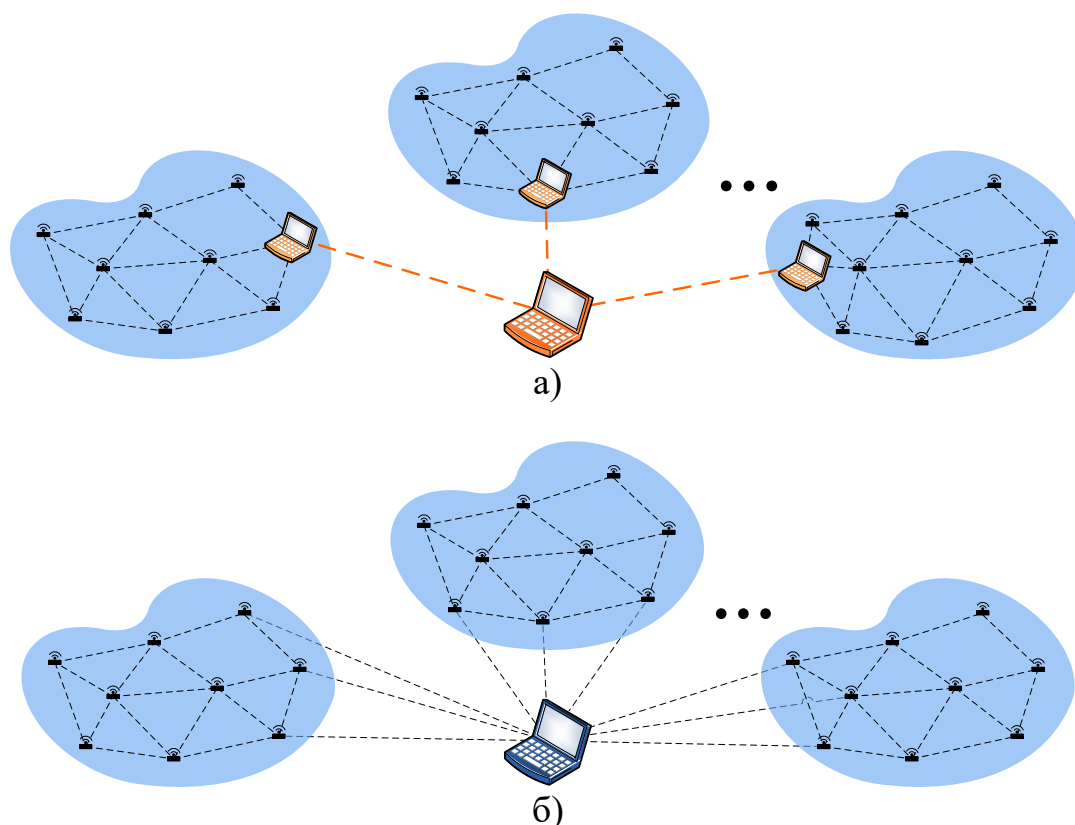
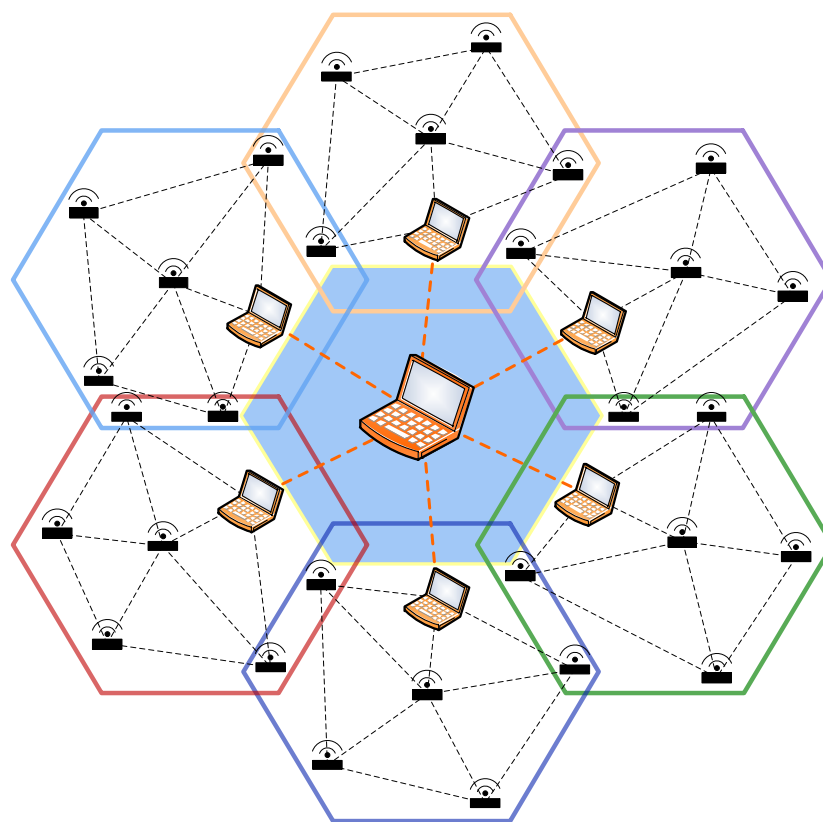
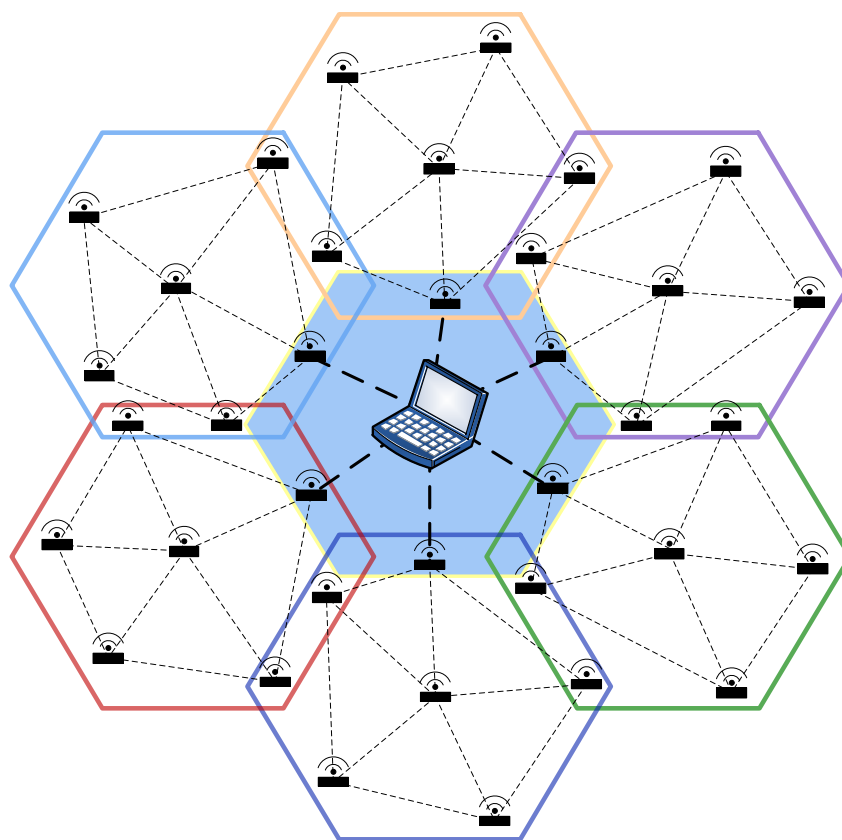


Рис. 8. Пример пространственной декомпозиции АСО разнесенных охраняемых периметров режимных объектов с иерархическим (а) и центральным одноуровневым (б) управлением



а)



б)

Рис. 9. Пример пространственной декомпозиции АСО охраняемых периметров режимных объектов с иерархическим (а) и центральным одноуровневым (б) управлением

При реализации данного способа дополнительным мероприятием защиты является проверка соответствия охранных извещений установленной зоне размещения охранных извещателей, а также проверка частотной (и другой) совместимости средств радиосвязи для различных зон.

Этап проверки (рис. 10) производится между блоками 3 и 4 блок-схемы алгоритма функционирования системы имитозащиты данных охранного извещателя, выполняющего функцию ретранслятора данных (рис. 6). Итогом проверки является либо дальнейшая обработка данных (в случае успешной проверки), либо инициализация сигнала «Тревога» (в противном случае), или стирание данных.

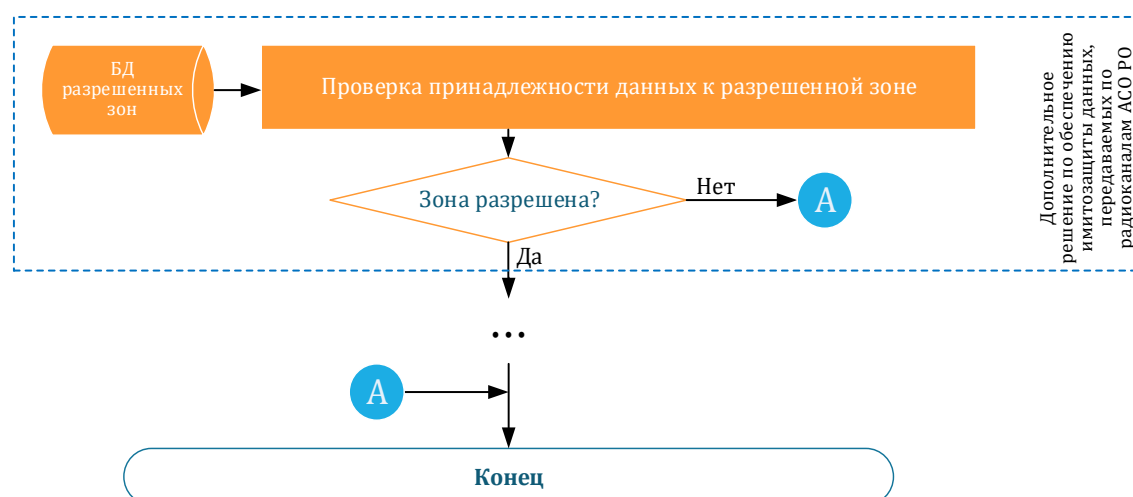


Рис. 10. Фрагмент алгоритма (добавочного шага) для проверки охранного извещателя, от которого поступило извещение, на принадлежность к разрешенной зоне (противодействие имитации на основе записи и повторов извещений и/или ретрансляции)

На этапе проверки поступивших данных ПЦН АСО РО выполняется контроль принадлежности извещателя, отправившего данные к соответствующей зоне. Этап проверки (рис. 10) выполняется с использованием данных о разрешенных зонах для соответствующих охранных извещателей (между блоками 3 и 4 блок-схемы алгоритма на рис. 7).

На рис. 11 представлен пример пространственной декомпозиции АСО пересекающихся охраняемых периметров РО с трехуровневым иерархическим управлением системой охраны. Данное решение направлено на обеспечение имитозащиты данных, циркулирующих между элементами системы охраны, разворачиваемой для организации охраны протяженных по площади режимных объектов и позволяет уменьшить вычислительную нагрузку на ПЦН АСО РО за счет разделения процессов проверки циркулирующих по сети данных на промежуточных этапах.

Шифрование служебных данных о состоянии охранного извещателя.

Дополнительной мерой защиты данных от имитационных воздействий злоумышленника, является шифрование служебных данных о состоянии охранного извещателя, инициирующего передачу данных по сети [33, 34].

Под служебными данными следует понимать сообщения (вариант):

- «Наблюдение» – сообщение, формируемое извещателем при функционировании системы охраны в штатном режиме;
- «Тревога» – сообщение, инициируемое извещателем при обнаружении несанкционированного проникновения нарушителя на охраняемый объект;
- «Аккумулятор» – сообщение, инициируемое извещателем при достижении заряда его аккумулятора критически низкого уровня.

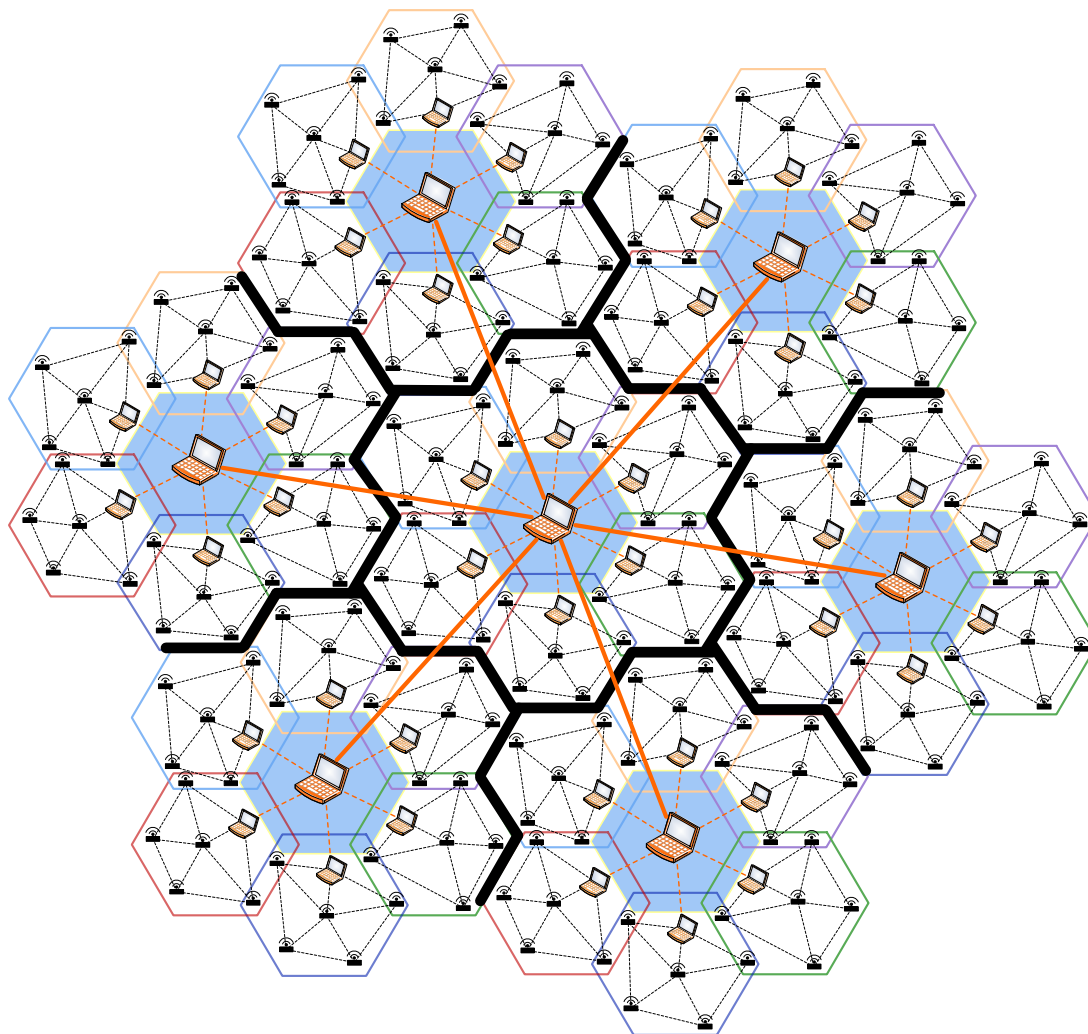


Рис. 11. Пример пространственной декомпозиции АСО охраняемых периметров РО с трехуровневым иерархическим управлением

Решение по шифрованию подлежащих передаче служебных данных является мерой, способной защитить АСО РО от таких деструктивных воздействий злоумышленника как запись и повтор ранее переданной информации с известными злоумышленнику параметрами работы охранных извещателей.

Рассмотрим порядок функционирования охранного извещателя АСО РО, инициирующего передачу служебных данных на ПЦН.

В охранном извещателе осуществляется хранение ключей:

$k_j^{(сл)}$ – ключ шифрования служебного сообщения о состоянии охранного извещателя;

k_j – ключ для вычисления имитовставки;

d_j – ключ подписи для вычисления ЭП;

e_j – ключ проверки ЭП данных, поступивших на извещатель.

Охранным извещателем с номером p формируется вектор $\mathbf{V}_p$, который содержит одно из трех служебных сообщений, дополненное меткой «*Unix Timestamp*» (последовательность символов, отражающих количество секунд, прошедших с 1 января 1970 года [35]). Это позволяет избежать выработки идентичных последовательностей служебных данных, подлежащих передаче и, тем самым, в условиях успешного перехвата злоумышленником служебных данных, не дать ему возможности повторно их использовать.

Алгоритм формирования служебных данных охранным извещателем, инициирующим передачу данных по сети можно представить в виде блок-схемы (рис. 12).

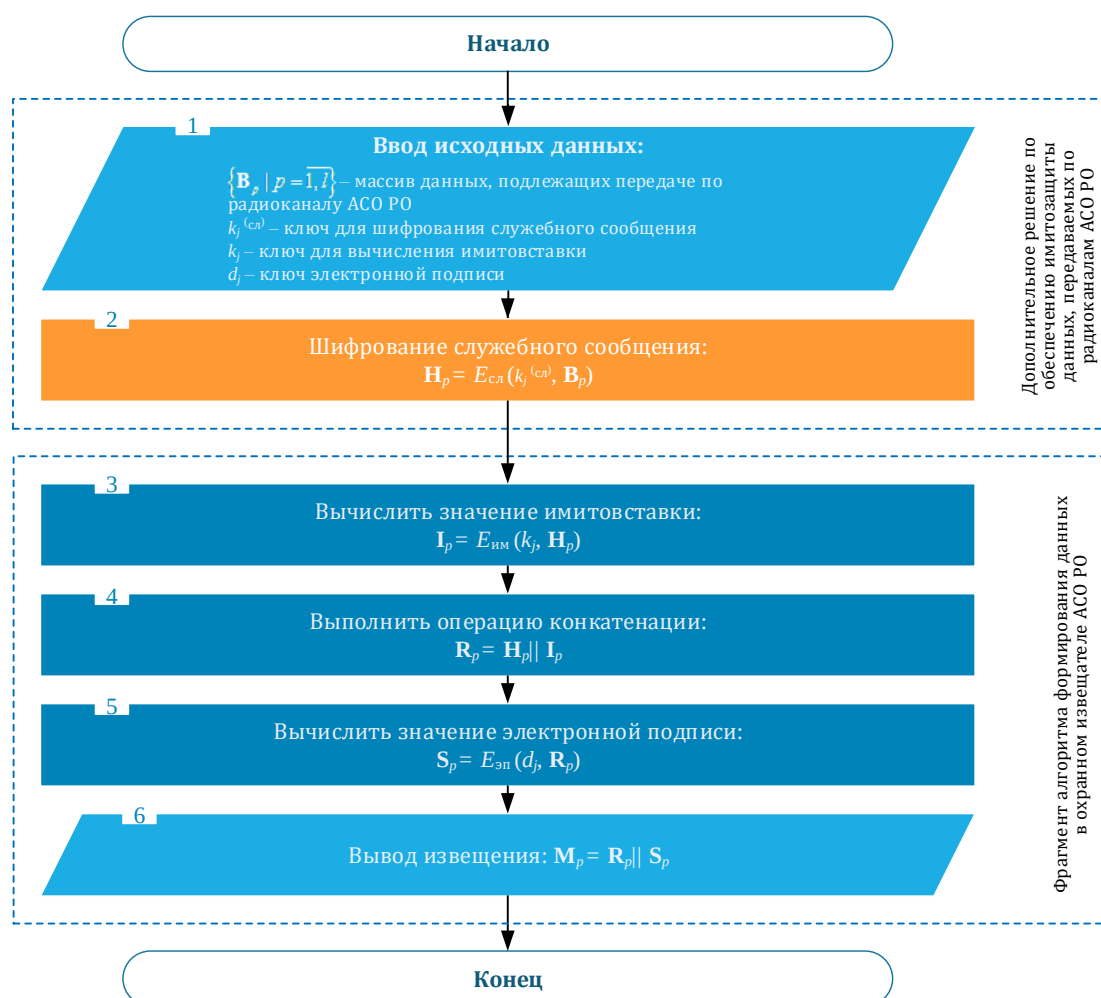


Рис. 12. Блок-схема алгоритма формирования данных в охранным извещателе АСО РО, инициирующим передачу данных по сети

Следующим этапом прохождения данных по сети АСО РО является проверка и формирование данных охранным извещателем, выполняющим функции ретранслятора. Следует заметить, что зашифрованное служебное сообщение о

состоянии охранного извещателя на этапе ретрансляции сообщения не контролируется, а подлежит проверке на ПЦН АСО РО.

На ПЦН осуществляется хранение:

БД ключей $k_j^{(сп)}$ для расшифрования служебного сообщения о состоянии охранного извещателя;

БД ключей k_j для вычисления имитовставки всех охранных извещателей, функционирующих в системе;

БД ключей e_j проверки подписи всех охранных извещателей, входящих в охранную систему.

Алгоритм функционирования системы имитозащиты данных ПЦН можно представить в виде блок-схемы (рис. 13). Решение по дополнительной криптографической защите информации, а именно введению дополнительного шифрования служебных данных, имеет целью внесение мер по обеспечению защиты данных от имитационных воздействий злоумышленника. Данное решение позволяет обеспечить защищенную циркуляцию служебных данных между элементами системы охраны в условиях активных действий злоумышленника, направленных на добывание и изучение структуры передаваемых данных с целью их дальнейшего использования в своих интересах.

Без применения дополнительных мер защиты злоумышленник, при наличии специального оборудования, имеет возможность изучать структуру служебных данных и использовать затем в деструктивных целях.

Формирование данных о характере имитационного воздействия. Рассмотрим случаи формирования сообщения о характере воздействий злоумышленника.

1. *Получение данных от охранного извещателя, не входящего в базу данных охранных извещателей.*

На каждом охранном извещателе, выполняющем функции ретранслятора и ПЦН выполняется проверка данных на соответствие БД легитимных извещателю. При обнаружении данных, сформированных охранным извещателем, не входящим в состав охранной системы, на ПЦН отправляется соответствующее сообщение. Алгоритм функционирования системы имитозащиты данных охранного извещателя, выполняющего функцию ретранслятора, и алгоритм функционирования системы имитозащиты данных ПЦН поясняется с помощью блок-схем (рис. 14, 15).

2. *Отрицательный результат проверки значения ЭП.*

В целях контроля подлинности поступивших данных охранными извещателями, выполняющими функции ретрансляторов сообщений, и ПЦН проверяется ЭП поступивших данных. Итогом проверки ЭП является либо разрешение дальнейшей обработки данных, либо инициализация сигнала «Тревога». При отрицательном результате проверки ЭП охранным извещателем – ретранслятором, может быть сформировано соответствующее сообщение для ПЦН АСО РО, либо выполнено стирание охранного извещения.

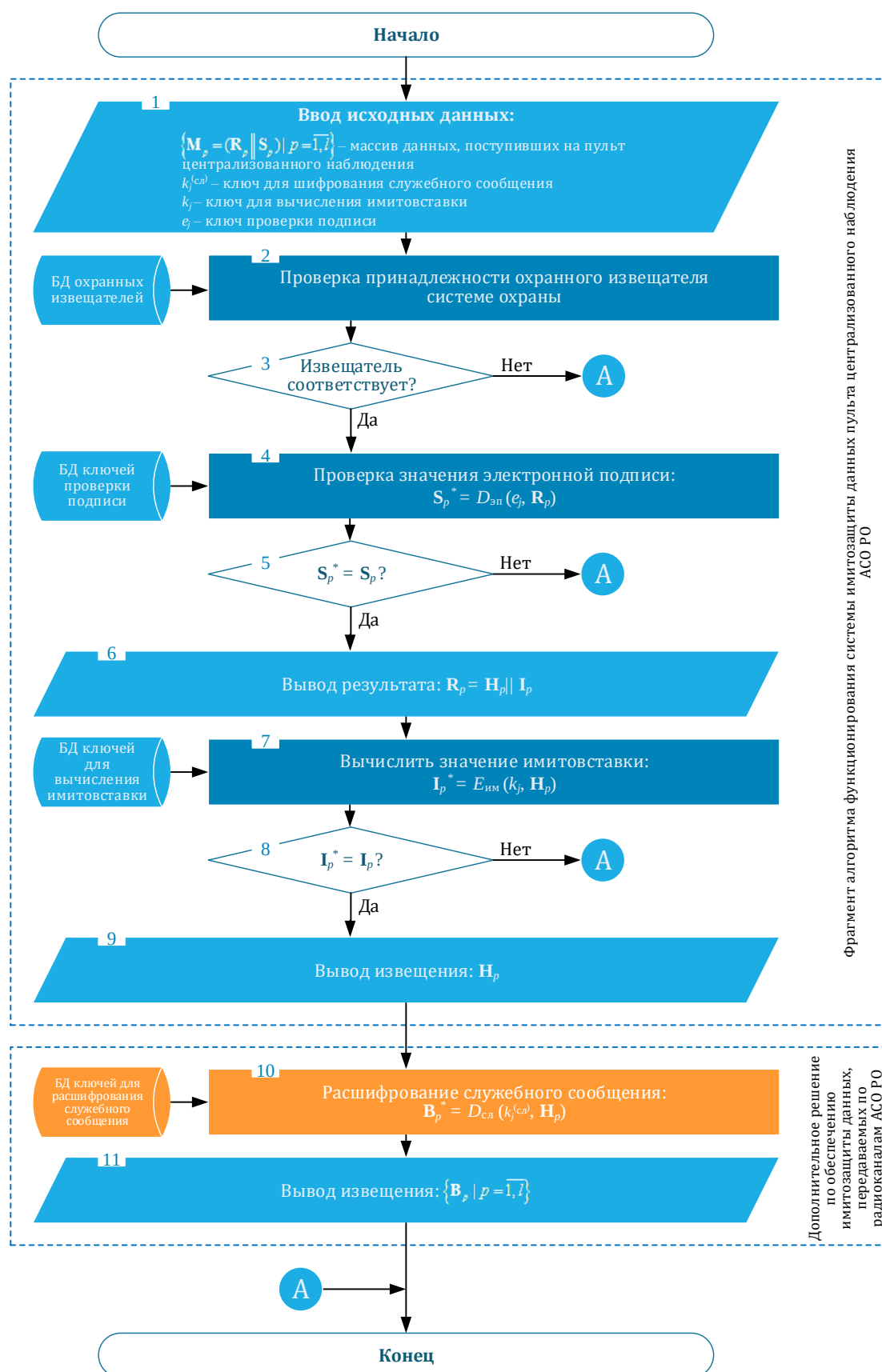


Рис. 13. Блок-схема алгоритма функционирования системы имитозащиты данных ПЦН АСО РО

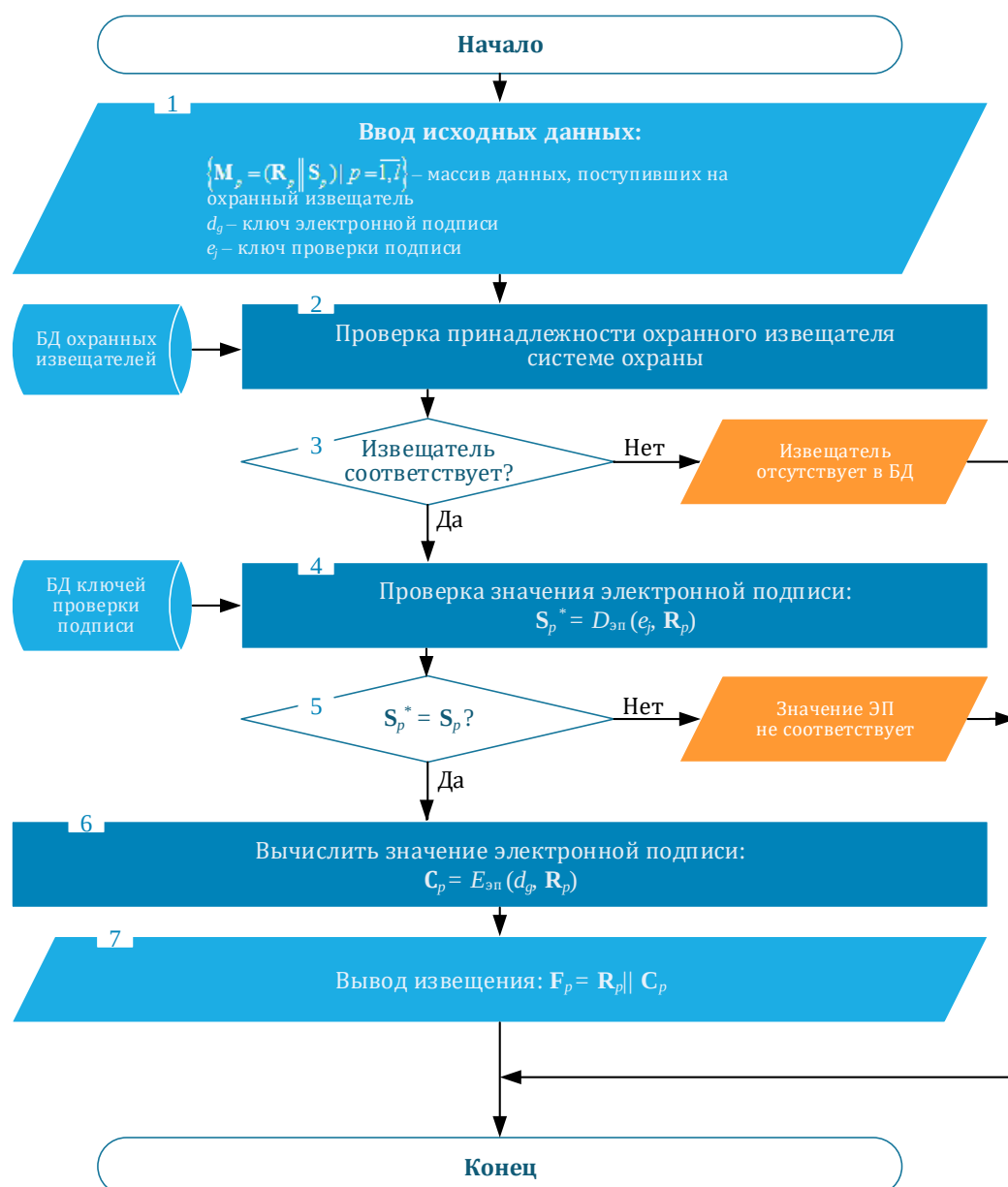


Рис. 14. Блок-схема алгоритма функционирования системы имитозащиты данных охранного извещателя, выполняющего функцию ретранслятора АСО РО

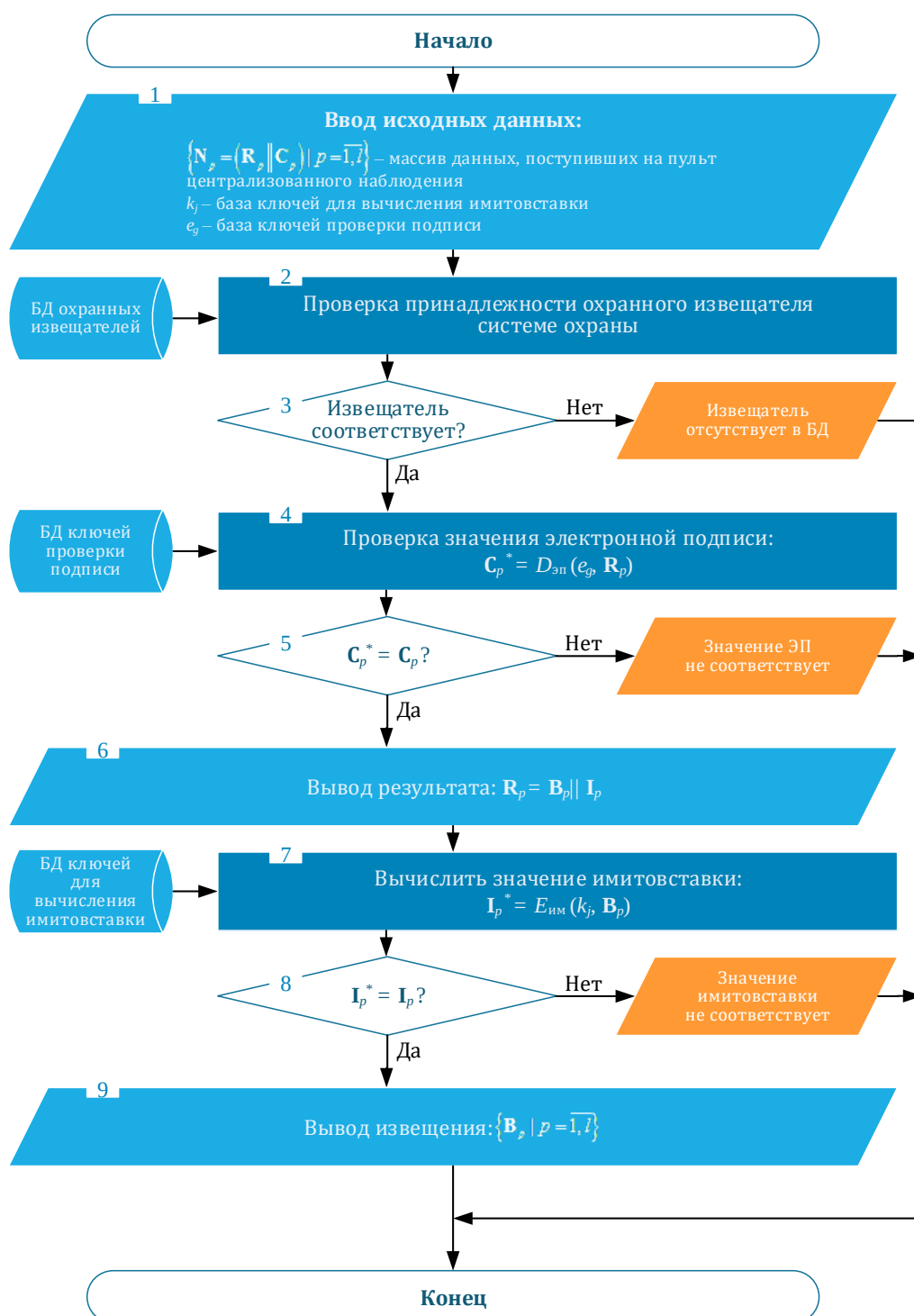


Рис. 15. Блок-схема алгоритма функционирования системы имитозащиты данных ПЦН АСО РО

Выработка и пролонгация действия криптографических ключей. Для обеспечения нормального функционирования подсистемы защиты информации АСО РО необходимо предусмотреть возможность выработки и пролонгации действия криптографических ключей [36], таких как:

$k_j^{(сл)}$ – ключ шифрования служебных сообщений о состоянии охранного извещателя;

k_j – ключ для вычисления имитовставки.

Выработку ключей охранным извещателем (параллельно с выработкой этих же ключей в ПЦН) предлагается производить путём шифрования (в соответствии с одним из стандартов) корневых ключей $k_j^{(сл)}$ и k_j , присвоенных ему администратором системы охраны. Вариант схемы выработки и пролонгации действия криптографических ключей представлена на рис. 16.

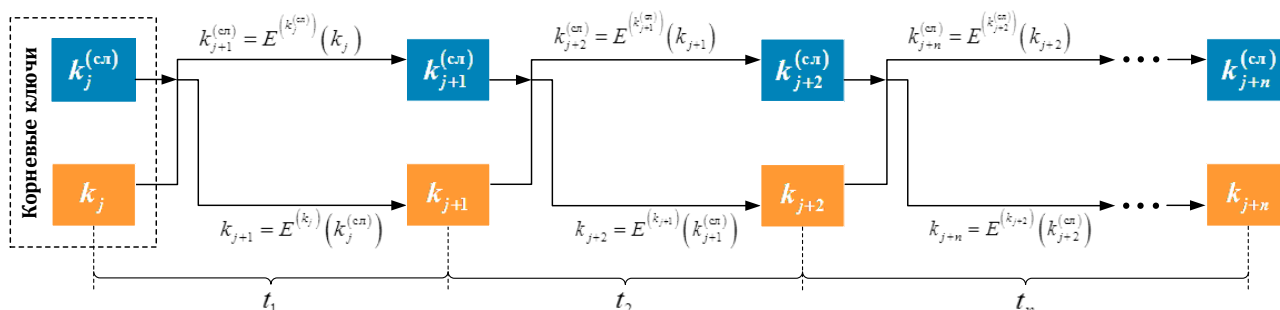


Рис. 16. Схема выработки и пролонгации действия криптографических ключей охранным извещателем АСО РО

Эти меры являются продолжением известных методов [37-39] и позволяют обеспечить имитозащиту данных за счет периодической автоматической смены ключей через определенные промежутки времени, либо принудительно, по распоряжению администратора (например, после посещения РО различных рабочих групп – инспекций или других лиц или техники).

Сигнализация несанкционированного доступа к охранному извещателю. В условиях свободного размещения охранных извещателей на местности, создаются благоприятные условия по беспрепятственному захвату охранных извещателей злоумышленником. Возникает необходимость обеспечения безопасного хранения криптографических ключей в памяти охранного извещателя.

Для этого конструкция извещателя дополняется датчиком контроля физической целостности корпуса извещателя (рис. 17). При несанкционированном вскрытии корпуса охранного извещателя следует экстренное стирание криптографических ключей. Также должен быть установлен контроль остаточного заряда основного аккумулятора извещателя и использование дополнительного аккумулятора для питания внутренних часов и вышеупомянутого датчика.

Оценивание защищенности беспроводной АСО РО

Для оценивания защищенности системы охраны рассмотрим состояния радиосети АСО РО с подсистемой защиты от имитационных воздействий злоумышленника и показатели вероятностей ее нахождения в различных состояниях [40–43].

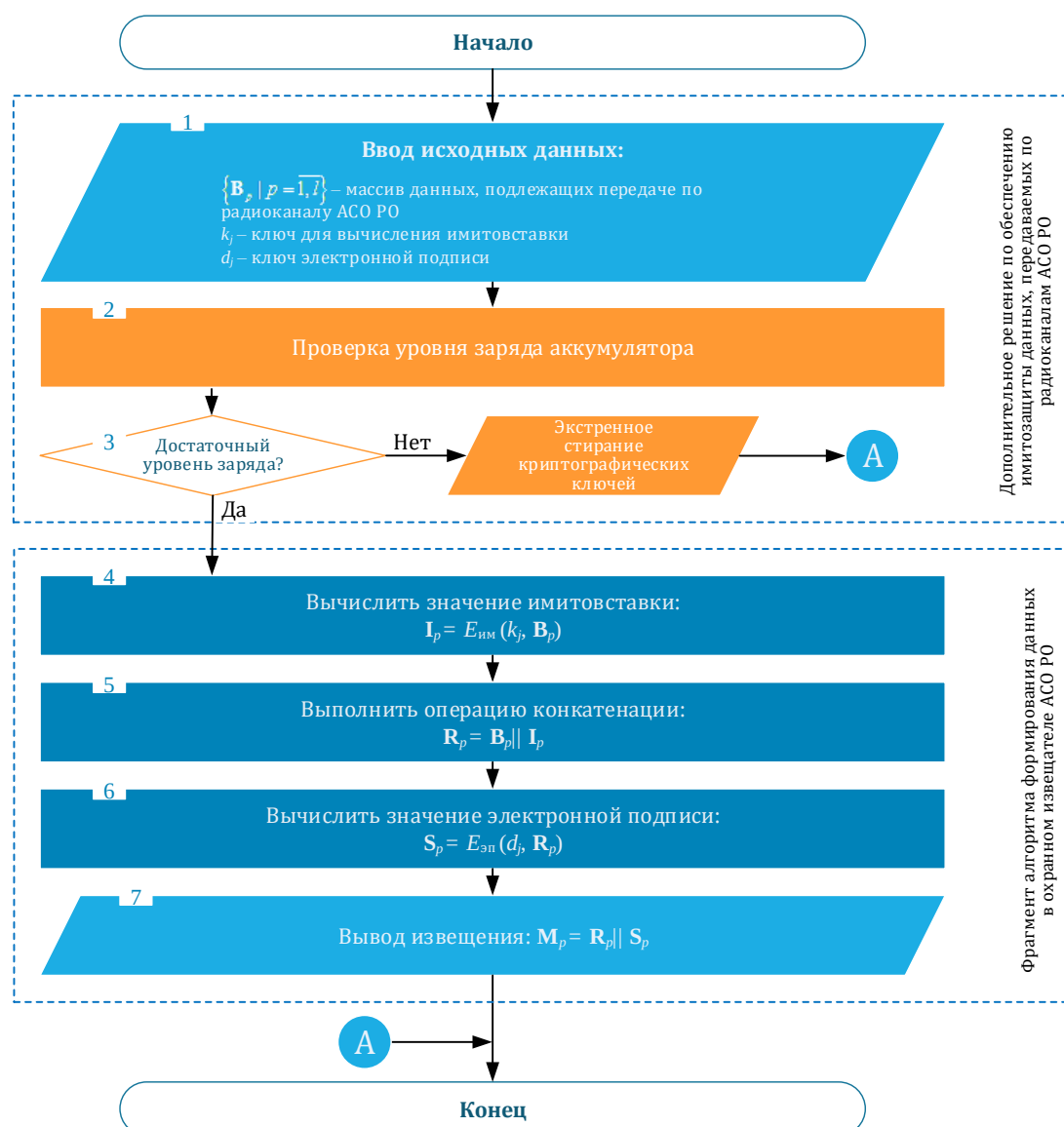


Рис. 17. Блок-схема алгоритма формирования данных в охранном извещателе АСО РО, инициирующим передачу данных по сети

Примем допущения:

- область искомых решений ограничивается канальным уровнем модели OSI; физический уровень не затрагивается;
- в качестве прототипа принято решение, основанное на выработке имитовставки или ключевой хеш-функции на общем секретном ключе.

Представим радиосеть АСО РО в виде модели (рис. 18) с дискретными состояниями в непрерывном времени [42]:

S_1 – состояние: «нормальное функционирование»;

S_2 – состояние: «явный отказ в обслуживании с долговременным устранением»;

S_3 – состояние: «явный отказ в обслуживании с самоустраниением»;

S_4 – состояние: «скрытый отказ в обслуживании – адресное инициирование ложных извещений»;

S_5 – состояние: «скрытый отказ в обслуживании – стирание легитимных извещений».

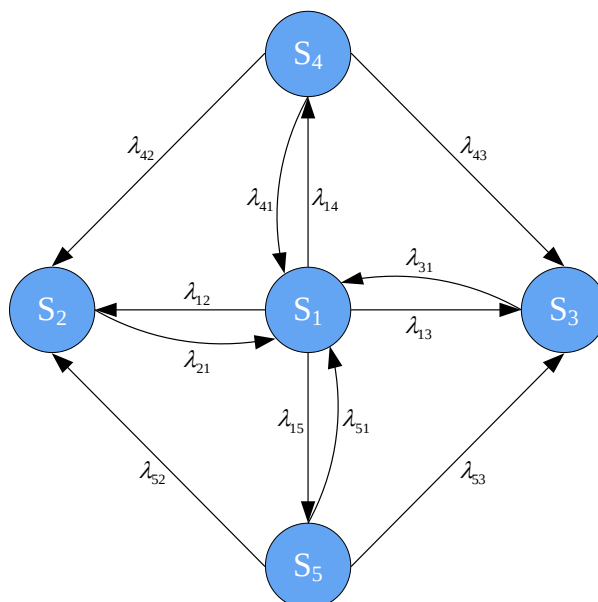


Рис. 18. Граф состояний радиосети АСО РО с подсистемой защиты от имитационных воздействий злоумышленника

Моменты возможных переходов системы из одного состояния в другое случайны и происходят под действием потоков событий, характеризующиеся их интенсивностями λ_{ab} , где $a, b = 1, \dots, 5$.

Система потоков событий с интенсивностями примет вид:

λ_{12} – компрометация критического количества криптографических ключей и/или преждевременный разряд батарей охранных извещателей в результате ее истощения имитацией;

λ_{13} – энергетическое подавление радиосети; массовая имитация злоумышленником сигнала «Тревога», а также массовая обнаруживаемая имитация ошибок 1-го или 2-го рода;

λ_{14} – искусственная адресная генерация ошибок 1-го или 2-го рода в работе одного или нескольких охранных извещателей (прямая имитация или создание ретрансляционной имитационной помехи);

λ_{15} – искусственная перегрузка сети путем инициирования ошибок 1-го или 2-го рода (принудительное «состаривание» меток времени легитимных сигналов для утраты их актуальности);

λ_{21} – возврат системы в состояние «нормальное функционирование» из состояния «явный отказ в обслуживании с долговременным устранением»;

λ_{31} – возврат системы в состояние «нормальное функционирование» из состояния «явный отказ в обслуживании с самоустраниением»;

λ_{41} – возврат системы в состояние «нормальное функционирование» из состояния «скрытый отказ в обслуживании – адресное инициирование ложных извещений»;

λ_{42} – «явный отказ в обслуживании с долговременным устранением» после адресного инициирования ложных извещений;

λ_{43} – «явный отказ в обслуживании с самоустраниением» после адресного инициирования ложных извещений;

λ_{51} – возврат системы в состояние «нормальное функционирование» из состояния «скрытый отказ в обслуживании – стирание легитимных извещений»;

λ_{52} – «явный отказ в обслуживании с долговременным устранением» после стирания легитимных извещений;

λ_{53} – «явный отказ в обслуживании с самоустраниением» после стирания легитимных извещений.

Вероятность $p_i(t)$ того, что в момент времени t система будет находиться в состоянии S_i , называется вероятностью i -го состояния. Граф состояний (рис. 18) можно описать системой дифференциальных уравнений Колмогорова [42, 43]:

$$\begin{cases} \frac{dp_1(t)}{dt} = \lambda_{21} \cdot p_2(t) + \lambda_{31} \cdot p_3(t) + \lambda_{41} \cdot p_4(t) + \lambda_{51} \cdot p_5(t) - (\lambda_{12} + \lambda_{13} + \lambda_{14} + \lambda_{15}) \cdot p_1(t); \\ \frac{dp_2(t)}{dt} = \lambda_{12} \cdot p_1(t) + \lambda_{42} \cdot p_4(t) + \lambda_{52} \cdot p_5(t) - \lambda_{21} \cdot p_2(t); \\ \frac{dp_3(t)}{dt} = \lambda_{13} \cdot p_1(t) + \lambda_{43} \cdot p_4(t) + \lambda_{53} \cdot p_5(t) - \lambda_{31} \cdot p_3(t); \\ \frac{dp_4(t)}{dt} = \lambda_{14} \cdot p_1(t) - (\lambda_{41} + \lambda_{42} + \lambda_{43}) \cdot p_4(t); \\ \frac{dp_5(t)}{dt} = \lambda_{15} \cdot p_1(t) - (\lambda_{51} + \lambda_{52} + \lambda_{53}) \cdot p_5(t); \\ \sum_{i=1}^5 p_i(t) = 1. \end{cases} \quad (3)$$

Для решения данной системы определим значения вероятностей начальных состояний:

$$p_1(0)=1, p_2(0)=0, \dots, p_5(0)=0. \quad (4)$$

Решение (3) будем осуществлять методом Рунге-Кутты четвертого порядка в условиях присвоения численных значений интенсивностям λ_{ab} и непрерывном времени $t \in [t_0, t_1]$ с фиксированным шагом интегрирования [42]:

$$\begin{cases} k_1^i = S(t_i, p_i), \\ k_2^i = S\left(t_i + \frac{h}{2}, p_i + \frac{h}{2}k_1^i\right), \\ k_3^i = S\left(t_i + \frac{h}{2}, p_i + \frac{h}{2}k_2^i\right), \\ k_4^i = S(t_i + h, p_i + hk_3^i), \\ \Delta p_i = \frac{h}{6}(k_1^i + 2k_2^i + 2k_3^i + k_4^i), \\ p_{i+1} = p_i + \Delta p_i, \end{cases} \quad (5)$$

где h – приращение, соответствующее шаговой поправке Эйлера, Δp_i – шаговая поправка (средневзвешенная величина поправок $hk_1^i, hk_2^i, hk_3^i, hk_4^i$ каждого этапа

интегрирования с весовыми коэффициентами $\frac{1}{6}, \frac{2}{6}, \frac{2}{6}, \frac{1}{6}$ соответственно) [42].

Приведем (3) к векторному виду:

$$\begin{bmatrix} \lambda_{21}p_2(t) + \lambda_{31}p_3(t) + \lambda_{41}p_4(t) + \lambda_{51}p_5(t) - (\lambda_{12} + \lambda_{13} + \lambda_{14} + \lambda_{15})p_1(t) \\ \lambda_{12}p_1(t) + \lambda_{42}p_4(t) + \lambda_{52}p_5(t) - \lambda_{21}p_2(t) \\ \lambda_{13}p_1(t) + \lambda_{43}p_4(t) + \lambda_{53}p_5(t) - \lambda_{31}p_3(t) \\ \lambda_{14}p_1(t) - (\lambda_{41} + \lambda_{42} + \lambda_{43})p_4(t) \\ \lambda_{15}p_1(t) - (\lambda_{51} + \lambda_{52} + \lambda_{53})p_5(t) \end{bmatrix} \quad (6)$$

Для решения (3) необходимо учитывать значения вероятностей начальных состояний системы, интервал интегрирования t_0, t_1 и число этапов интегрирования n . На этапе решения производится расчет для заданных значений интенсивностей событий $\lambda_{ab} = \text{const}$ (марковский однородный процесс), что позволяет получить числовую таблицу приближенных значений p_i искомых решений $p(t)$ на некотором интервале $t \in [t_0, t_1]$ для вариантов построения В 2 и В 3:

В 2 – сеть строится на основе применения распределенной структуры с ячеистой топологией, где все охранные извещатели снабжаются единым (для всей сети) секретным ключом, необходимым для формирования имитовставки или ключевой хеш-функции.

В 3 – сеть строится в соответствии с В 2 и дополнительно все охранные извещатели сети снабжаются индивидуальными секретными ключами, необходимыми для выработки имитовставок для аутентификации отправляемых извещений.

Определим исходные данные (таблица 1).

Интенсивность перехода состояний:

$$\lambda_{ab}(t) = \lim_{\Delta t \rightarrow 0} \frac{p_{ab}(t, t + \Delta t)}{\Delta t}, \text{ где } a \neq b.$$

В качестве примера для определения значений переходных вероятностей p_{ab} каждого из состояний системы воспользуемся численными значениями, определенных охранному комплексу «Радиобарьер» [1]:

$$P_{\text{обн}}=0,9; P_{\text{лс}}=0,012; P_{\text{прон}}=0,1.$$

Вероятность компрометации ключа одного охранного извещателя (полный перебор ключа имитовставки):

$$P_{\text{компромет}} = 2^{-n},$$

где n – длина криптографического ключа.

Под численными значениями вероятностей компрометации сети будем использовать значения, вычисленные по формулам (1) и (2) для систем, построенных по варианту В 2 и В 3 соответственно.

Рассмотрим радиосеть АСО РО в соответствии с вариантом В 2 при заданных значениях интенсивностей (таблица 1) на интервале $t \in [0, 1800]$ и числом этапов интегрирования $n = 3600$.

Таблица 1 – Значения интенсивностей переходов системы

Интенсивность	λ_{ab}	Значения λ_{ab} для различных вариантов	
		В 2	В 3
Компрометация критического количества криптографических ключей АСО РО и/или преждевременный разряд батарей	λ_{12}	3	1
Энергетическое подавление радиосети; массовая имитация сигнала «Тревога», а также массовая обнаруживаемая имитация ошибок 1-го или 2-го рода	λ_{13}	3	1
Искусственная адресная генерация ошибок 1-го или 2-го рода в работе одного или нескольких охранных извещателей	λ_{14}	3	1
Искусственная перегрузка сети путем инициирования ошибок 1-го или 2-го рода	λ_{15}	3	1
Возврат системы в состояние «нормальное функционирование» из состояния «явный отказ в обслуживании с долговременным устранением»	λ_{21}	0,17	0,81
Возврат системы в состояние «нормальное функционирование» из состояния «явный отказ в обслуживании с самоустранением»	λ_{31}	$6,1 \cdot 10^{-8}$	$1,52 \cdot 10^{-5}$
Возврат системы в состояние «нормальное функционирование» из состояния «скрытый отказ в обслуживании – адресное инициирование ложных извещений»	λ_{41}	$6,1 \cdot 10^{-8}$	$1,83 \cdot 10^{-8}$
Состояние «явный отказ в обслуживании с долговременным устранением»	λ_{42}	$5,08 \cdot 10^{-5}$	$1,83 \cdot 10^{-8}$
Состояние «явный отказ в обслуживании с самоустранением»	λ_{43}	$1,52 \cdot 10^{-5}$	$1,83 \cdot 10^{-8}$
Возврат системы в состояние «нормальное функционирование» из состояния «скрытый отказ в обслуживании – стирание легитимных извещений»	λ_{51}	$6,1 \cdot 10^{-8}$	$1,52 \cdot 10^{-5}$
Состояние «явный отказ в обслуживании с долговременным устранением»	λ_{52}	$5,08 \cdot 10^{-5}$	$4,67 \cdot 10^{-5}$
Состояние «явный отказ в обслуживании с самоустранением»	λ_{53}	0,07	$1,52 \cdot 10^{-5}$

Система (6) примет вид:

$$\begin{bmatrix} 0.17 p_2(t) + 6.1 \cdot 10^{-8} p_3(t) + 6.1 \cdot 10^{-8} p_4(t) + 6.1 \cdot 10^{-8} p_5(t) - (3 + 3 + 3 + 3) p_1(t) \\ 3 p_1(t) + 5.08 \cdot 10^{-5} p_4(t) + 5.08 \cdot 10^{-5} p_5(t) - 0.17 p_2(t) \\ 3 p_1(t) + 1.52 \cdot 10^{-5} p_4(t) + 0.07 p_5(t) - 6.1 \cdot 10^{-8} p_3(t) \\ 3 p_1(t) - (6.1 \cdot 10^{-8} + 5.08 \cdot 10^{-5} + 1.52 \cdot 10^{-5}) p_4(t) \\ 3 p_1(t) - (6.1 \cdot 10^{-8} + 5.08 \cdot 10^{-5} + 0.07) p_5(t) \end{bmatrix}$$

Приближенные значения p_i представлены в таблице 2.

Таблица 2 – Приближенные значения p_i для состояний системы, при построении сети по варианту В 2

Этап интегрирования	$p(t)$				
	$p_1(t)$	$p_2(t)$	$p_3(t)$	$p_4(t)$	$p_5(t)$
1	1	0	0	0	0
2	0,996	0,001	0,001	0,001	0,001
3	0,995	0,001	0,001	0,001	0,002
4	0,992	0,002	0,002	0,002	0,002
5	0,989	0,003	0,002	0,003	0,003
...	...	...	...	...	...
3600	0,003	0,221	0,254	0,259	0,263

Полученные значения: $p_1(t)=0,003$, $p_2(t)=0,221$, $p_3(t)=0,254$, $p_4(t)=0,259$ и $p_5(t)=0,263$ указывают на конечные значения вероятностей нахождения системы в каждом из рассматриваемых состояний.

В целях дальнейшего оценивания защищенности системы охраны, рассмотрим процесс функционирования АСО РО для варианта В 3 при заданных значениях интенсивностей (таблица 1) на интервале $t \in [0, 1800]$ и тем же числом этапов, что и предыдущем варианте.

Система (6) примет вид:

$$\begin{bmatrix} 0.81 p_2(t) + 1.52 \cdot 10^{-5} p_3(t) + 1.83 \cdot 10^{-8} p_4(t) + 1.52 \cdot 10^{-5} p_5(t) - (1 + 1 + 1 + 1) p_1(t) \\ p_1(t) + 1.83 \cdot 10^{-8} p_4(t) + 4.67 \cdot 10^{-5} p_5(t) - 0.81 p_2(t) \\ p_1(t) + 1.83 \cdot 10^{-8} p_4(t) + 1.52 \cdot 10^{-5} p_5(t) - 1.52 \cdot 10^{-5} p_3(t) \\ p_1(t) - (1.83 \cdot 10^{-8} + 1.83 \cdot 10^{-8} + 1.83 \cdot 10^{-8}) p_4(t) \\ p_1(t) - (1.52 \cdot 10^{-5} + 4.67 \cdot 10^{-5} + 1.52 \cdot 10^{-5}) p_5(t) \end{bmatrix}$$

Приближенные значений p_i представлены в таблице 3.

Таблица 3 – Приближенные значения p_i для состояний системы, при построении сети по варианту В 3

Этап интегрирования	$p(t)$				
	$p_1(t)$	$p_2(t)$	$p_3(t)$	$p_4(t)$	$p_5(t)$
1	1	0	0	0	0
2	0,996	0,001	0,001	0,001	0,001
3	0,996	0,001	0,001	0,001	0,001
4	0,993	0,001	0,002	0,002	0,002
5	0,991	0,002	0,002	0,002	0,003
...	...	...	...	...	...
3600	0,115	0,151	0,239	0,244	0,251

Полученные значения: $p_1(t)=0,115$, $p_2(t)=0,151$, $p_3(t)=0,239$, $p_4(t)=0,244$ и $p_5(t)=0,251$ указывают на конечные значения вероятностей нахождения системы в каждом из рассматриваемых состояний.

Из анализа таблиц 2 и 3 следует, что в целях более полного оценивания защищенности системы целесообразно рассмотреть поведение АСО РО в состояниях: S_1 – «нормальное функционирование», S_2 – «явный отказ в обслуживании с долговременным устранением» и S_4 – «скрытый отказ в обслуживании – адресное инициирование ложных извещений» в условиях различных вариантов построения сети (В 2 и В 3). Рассмотрение состояний системы S_3 и S_5 целесообразно опустить ввиду схожести значений вероятностей со значениями состояний S_2 и S_4 соответственно.

Получим коэффициент выигрыша $K_{\text{выигр.}}$ для каждого из возможных состояний радиосети АСО РО ($S_1 - S_5$):

$$K_{\text{выигр.}} = \frac{A_1^{(S_i)}}{A_2^{(S_i)}}, \quad (7)$$

где $A_1^{(S_i)}$ – сумма значений вероятностей нахождения системы в состоянии S_i на интервале времени $t \in [0, 1800]$ при построении сети по варианту В 2, $A_2^{(S_i)}$ – сумма значений вероятностей нахождения системы в состоянии S_i на интервале времени $t \in [0, 1800]$ при построении сети по варианту В 3.

На рис. 19-21 представлены зависимости значений вероятностей нахождения радиосети АСО РО в состояниях S_1 – «нормальное функционирование», S_2 – «явный отказ в обслуживании с долговременным устранением» и S_4 – «скрытый отказ в обслуживании – адресное инициирование ложных извещений» от времени ее функционирования при вариантах построения сети В 2 и В 3.

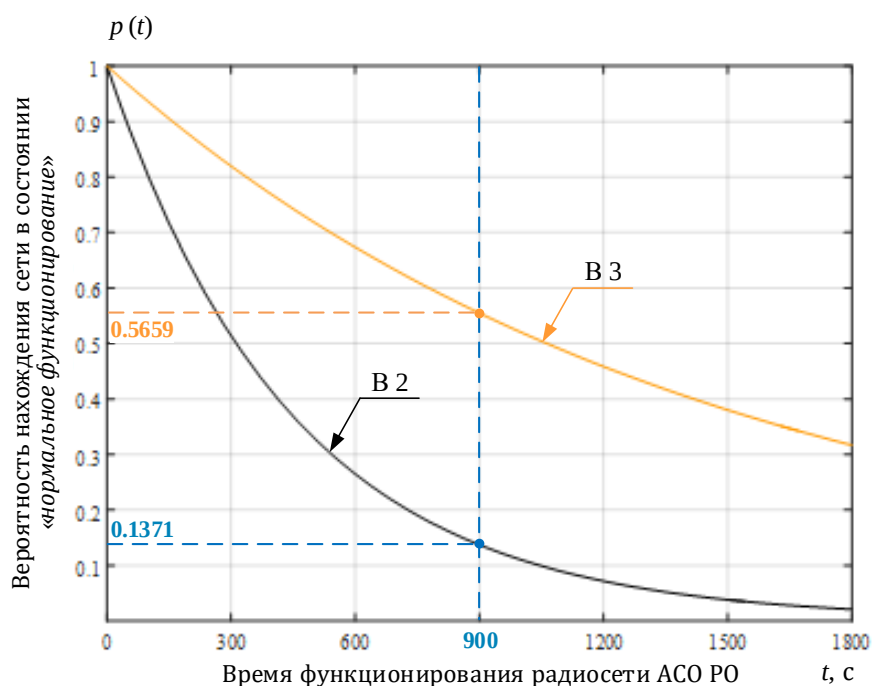


Рис. 19. Зависимость вероятности нахождения радиосети АСО РО в состоянии «нормальное функционирование» от времени ее функционирования при вариантах построения сети В 2 и В 3

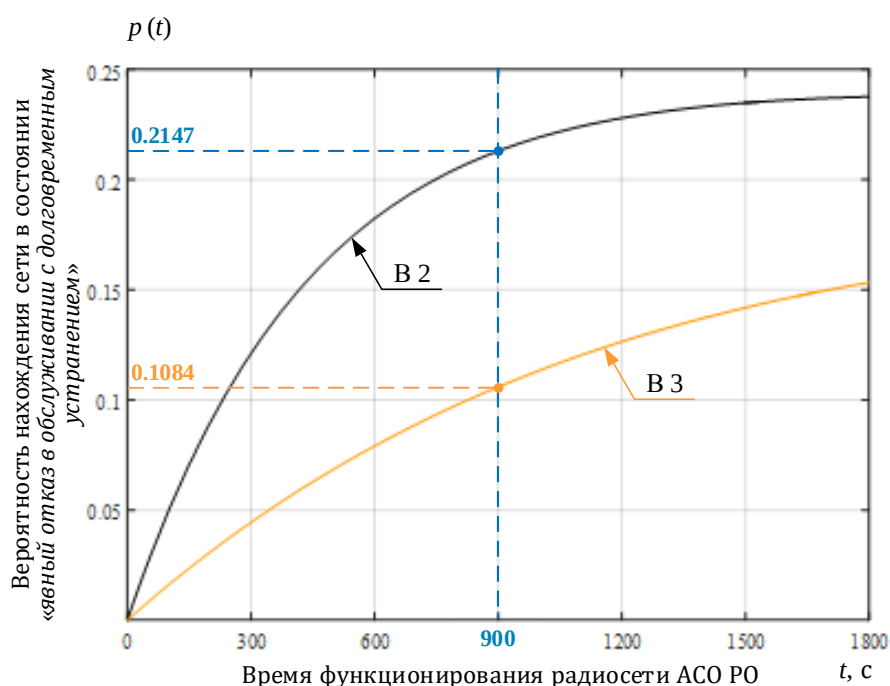


Рис. 20. Зависимость вероятности нахождения радиосети АСО РО в состоянии «явный отказ в обслуживании с долговременным устранением» от времени ее функционирования при вариантах построения сети В 2 и В 3

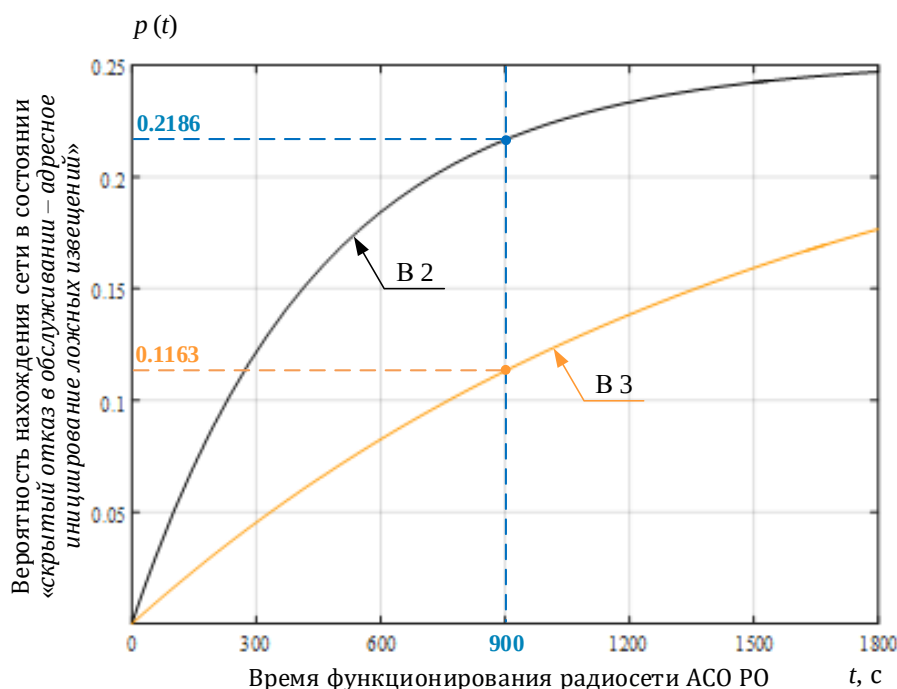


Рис. 21. Зависимость вероятности нахождения радиосети АСО РО в состоянии «скрытый отказ в обслуживании – адресное инициирование ложных извещений» от времени ее функционирования при вариантах построения сети В 2 и В 3

Выводы

Разработан комплекс алгоритмов имитозащиты данных, передаваемых по радиоканалам АСО РО, позволяющий повысить уровень защищенности сигнализационных (извещательных) данных. Оригинальность предложенных алгоритмов и методики заключается в использовании новых правил и приёмов комплексирования известных криптографических алгоритмов и протоколов, а также различных режимов функционирования.

Показано, что при использовании предлагаемых алгоритмов:

- возрастает вероятность ($\approx 14\%$) нахождения АСО РО в состоянии «нормальное функционирование» при варианте построения сети В 3;
- уменьшается вероятность ($\approx 28\%$) нахождения радиосети АСО РО в состоянии «явный отказ в обслуживании с долговременным устранением» при варианте построения сети В 3;
- уменьшается вероятность ($\approx 16\%$) нахождения радиосети АСО РО в состоянии «скрытый отказ в обслуживании – адресное инициирование ложных извещений».

Дальнейшие исследования предполагают:

- улучшение полноты и точности оценивания эффективности АСО РО за счёт учёта ошибок срабатывания охранных извещателей 1-го и 2-го рода *непредумышленного происхождения*;
- построение интеллектуальной системы поддержки принятия решений оператором АСО РО за счёт анализа служебных данных об имитационных действиях злоумышленника.

Литература

1. Андреев А. С., Степанов С. В. Автоматизированные системы охраны ракетных комплексов: учебное пособие. – Серпухов: Военная академия ракетных войск стратегического назначения имени Петра Великого (филиал в г. Серпухове), 2015. – 321 с.
2. Севрюков Д. В., Асфандияров А. Х. Системы физической защиты объектов ядерной энергетики // Безопасность окружающей среды: Безопасность ядерных и радиационных объектов. 2007. № 3. С. 12-17.
3. О перечне сведений, отнесенных к государственной тайне. Указ Президента Российской Федерации от 24 января 1998 г. № 61 (с изменениями на 8 июня 2020 года) // Официальное интернет-представительство президента России [Электронный ресурс]. 2020. – URL: <http://www.kremlin.ru/acts/bank/11915> (дата обращения: 15.06.2020).
4. Dargie W., Poellabauer C. Fundamentals of Wireless Sensor Networks: Theory and Practice. – John Wiley and Sons, 2010. – 330 p.
5. Cao L., Zhou S. Intelligent Security System Based on Wireless Sensor Networks. – First International Conference on Intelligent Networks and Intelligent Systems, 2008. – pp. 143-146. doi: 10.1109/ICINIS.2008.17.
6. Лихтциндер Б. Я., Киричек Р. В., Федотов Е. Д., Голубничая Е. Ю., Кочуров А. А. Беспроводные сенсорные сети: учебное пособие. – М.: Горячая линия-Телеком, 2020. – 236 с.
7. Дудолодов В. А., Минаев В. А., Севрюков Д. В., Сычев М. П., Еремеев С. А. О современных радиоканальных системах безопасности // Актуальные проблемы деятельности подразделений УИС. 2017. С. 225-229.
8. Шемигон Н. Н. Использование средств криптографической защиты информации в сетях связи систем физической защиты ядерно-опасных объектов // Связь и автоматизация МВД России. 2004. № 1. С. 48-51.
9. Брауде-Золотарев Ю. М., Максимов С. А., Руднев А. Н., Соколов Е. Е. Защита каналов технических средств охраны // Системы безопасности. 2002. № 5. С. 64-66.
10. Давыдов Ю. Л. Имитостойкие радиоканалы технических средств охраны // Транспортная безопасность и технологии. 2007. № 4. С. 33.
11. Samoylenko D. V., Ereemeev M. A. Finko O. A. A method of providing the integrity of information in the group of robotic engineering complexes based on crypt-code constructions // Automatic Control and Computer Sciences. 2017. Vol. 51. P. 965-971. doi: 10.3103/S0146411617080181.
12. Samoylenko D., Ereemeev M., Finko O., Dichenko S. Protection of Information from Imitation on the Basis of Crypt-Code Structures // Advances in Soft and Hard Computing. ACS 2018. Advances in Intelligent Systems and Computing. Springer. Cham. 2019. Vol. 889. P. 317-331. doi: 10.1007/978-3-030-03314-9_28.
13. Глобин Ю. О., Финько О. А. Способ обеспечения имитостойчивой передачи информации по каналам связи // Научные технологии в космических исследованиях Земли. 2020. Т. 12. № 2. С. 30-43. doi: 10.36724/2409-5419-2020-12-2-30-43.

14. Брауде-Золотарев Ю. В. Алгоритмы безопасности радиоканалов // Алгоритм безопасности. 2013. № 1. С. 64-66.
15. Василевский В. В., Завьялов С. А. Способ передачи извещений для систем централизованной радиоохраны // Омский научный вестник. 2010. № 2. С. 203-206.
16. Wang Y., Attebury G., Ramamurthy B. A Survey of Security Issues in Wireless Sensor Networks. – IEEE Communications Surveys and Tutorials, 2006. – pp. 2-23. doi: 10.1109/COMST.2006.315852.
17. Kibirige G., Sanga C. Attacks in Wireless Sensor Networks. – Sensor Technology: Concepts, Methodologies, Tools and Applications, 2020. – pp. 1215-1232. doi: 10.4018/978-1-7998-2454-1.ch058.
18. Bilal M., Kang S.-G. An Authentication Protocol for Future Sensor Networks. – Sensors, 2017. – pp. 1-29. doi:10.3390/s17050979.
19. Yoo S.-G., Park K.-Y., Kim J. A Security-Performance-Balanced User Authentication Scheme for Wireless Sensor Networks. – International Journal of Distributed Sensor Networks, 2012. – pp. 1-11. doi:10.1155/2012/382810.
20. Zhang J., Varadharajan V. Wireless Sensor Network Key Management Survey and Taxonomy. – Journal of Network and Computer Applications, 2010. – pp. 63-75. doi: 10.1016/j.jnca.2009.10.001.
21. Wang Y., Attebury G., Ramamurthy B. A Survey of Security Issues in Wireless Sensor Networks. – IEEE Communications Surveys and Tutorials, 2006. – pp. 2-23. doi: 10.1109/COMST.2006.315852.
22. Bilal M., Kang S.-G. Time-Assisted Authentication Protocol. – International Journal of Communication Systems, 2017. – pp. 27-33.
23. Kumar P., Gurtov A., Ylianttila M., Lee S.-G., Lee H.-G. A Strong Authentication Scheme with User Privacy for Wireless Sensor Networks. – ETRI Journal, 2013. – pp. 889-899. doi: 10.4218/etrij.13.0113.0103.
24. Choi Y., Lee Y., Won D. Cryptanalysis on Symmetric Key Techniques Based Authentication Scheme for Wireless Sensor Networks. – Computer Science and Ubiquitous Computing, 2015. – pp. 7-13.
25. Zhou Y., Fang Y. Defend Against Topological Attacks in Sensor Networks. – IEEE Military Communications Conference, 2006. – pp. 1-6. doi: 10.1109/MILCOM.2005.1605774.
26. Оленин Ю. А. Основы систем безопасности объектов: учебное пособие. – Пенза: Пензенский государственный университет, 2002. – 118 с.
27. ГОСТ Р 50922–2006 Защита информации. Основные термины и определения. – М.: Стандартинформ, 2006. – 8 с.
28. ISO/IEC 7498-1:1994. Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model. – ISO/IEC JTC 1, 1996. – 59 p.
29. Банк данных угроз безопасности информации // Официальный сайт ФСТЭК России» [Электронный ресурс]. 2020. – URL: <https://bdu.fstec.ru/threat> (дата обращения: 10.06.2020).
30. ГОСТ Р 34.13–2015 Криптографическая защита информации. Режимы работы блочных шифров. – М.: Стандартинформ, 2015. – 23 с.

31. Bashurov V. V., Filimonenkov V. O., Yaroslavtsev A. A., Churikov Yu. I. Problem of Territory Security // Journal of nuclear materials management. USA. Fall, 2004. P. 31-32.
32. Макаренко С. И., Рюмшин К. Ю., Михайлов Р. Л. Модель функционирования объекта сети связи в условиях ограниченной надежности каналов связи // Информационные системы и технологии. 2014. № 6 (86). С. 139-147.
33. Р 1323565.1.006–2017. Информационная технология. Криптографическая защита информации. Механизмы выработки псевдослучайных последовательностей. – М.: Стандартинформ, 2017. – 7 с.
34. МР 26.2.003–2014. Информационная технология. Криптографическая защита информации. Механизмы выработки псевдослучайных последовательностей. – М.: Технический комитет по стандартизации, 2014. – 8 с.
35. Грекул В. И., Денищенко Г. Н., Коровкина Н. Л. Проектирование информационных систем: учебное пособие. – М.: Бином, 2012. – 299 с.
36. МР 26.2.002–2016. Информационная технология. Криптографическая защита информации. Криптографические алгоритмы выработки ключей шифрования информации и аутентификационных векторов, предназначенных для реализации в аппаратных модулях доверия для использования в подвижной радиотелефонной связи. – М.: Технический комитет по стандартизации, 2016. – 13 с.
37. Самойленко Д. В., Еремеев М. А., Финько О. А., Диченко С. А. Параллельный линейный генератор многозначных псевдослучайных последовательностей с контролем ошибок функционирования // Труды СПИИРАН. 2018. № 4 (59). С. 31-61. doi: 10.15622/sp.59.2.
38. Finko O., Samoylenko D., Dichenko S, Eliseev N. Parallel generator of q-valued pseudorandom sequences based on arithmetic polynomials // Przegląd Elektrotechniczny. 2015. Vol. 3. № 91. P. 24-27. doi: 10.15199/48.2015.03.06.
39. Finko O., Dichenko S. Secure Pseudo-Random Linear Binary Sequences Generators Based on Arithmetic Polynoms // Soft Computing in Computer and Information Science. 2015. Vol. 342. P. 279-290. doi: 10.1007/978-3-319-15147-2_24.
40. Вентцель Е. С. Теория вероятностей. – М.: Академия, 2003. – 576 с.
41. Гмурман В. Е. Теория вероятностей и математическая статистика. – М.: Юрайт, 2013. – 479 с.
42. Вержбицкий В. М. Основы численных методов: учебник для вузов. – М.: Высшая школа, 2002. – 840 с.
43. Колмогоров А. Н., Журбенко И. Г., Прохоров А. В. Введение в теорию вероятностей. – М.: Наука, 1982. – 160 с.

References

1. Andreev A. S., Stepanov S. V. *Avtomatizirovannye sistemy ohrany raketnykh kompleksov* [Automated Missile Defense Systems]. Serpuhov, Peter the Great Military Academy of Strategic Rocket Forces (Branch in Serpuhov) Publ., 2015, 321 p. (in Russian).

2. Sevrjukov D. V., Asfandijarov A. X. Physical protection systems of nuclear power in stallations. *Environmental Safety: Safety of nuclear and radiation objects*, 2007, No. 3, Pp. 12-17 (in Russian).

3. O perechne svedenij, otnesennyh k gosudarstvennoj tajne. Ukaz Prezidenta Rossijskoj Federacii ot 24 janvarja 1998 g. № 61 (s izmenenijami na 8 ijunja 2020 goda) [On the list of information classified as state secret. Decree of the President of the Russian Federation of January 24, 1998 no. 61]. *Oficial'noe internet-predstavitel'stvo prezidenta Rossii* [The official website of the President of Russia], 15 June 2020. Available at: <http://www.kremlin.ru/acts/bank/11915> (accessed 15 June 2020) (in Russian).

4. Dargie W., Poellabauer C. *Fundamentals of Wireless Sensor Networks: Theory and Practice*. John Wiley and Sons, 2010. 330 p.

5. Cao L., Zhou S. *Intelligent Security System Based on Wireless Sensor Networks*. First International Conference on Intelligent Networks and Intelligent Systems, 2008. pp. 143-146. doi: 10.1109/ICINIS.2008.17.

6. Lihtcinder B. Ja., Kirichek R. V., Fedotov E. D., Golubnichaja E. Ju., Kochurov A. A. *Besprovodnye sensornye seti* [Wireless Sensor Networks]. Moscow, Gorjachaja Linija-Telekom Publ., 2020. 236 p (in Russian).

7. Dudoladov V. A., Minaev V. A., Sevrjukov D. V., Sychev M. P., Eremeev S. A. O sovremennyh radiokanal'nyh sistemah bezopasnosti [About modern radio security systems]. *Aktual'nye problemy dejatel'nosti podrazdelenij UIS*, 2017, pp. 225-229 (in Russian).

8. Shemigon N. N. Ispol'zovanie sredstv kriptograficheskoy zashhity informacii v setjah svjazi system fizicheskoy zashhity jaderno-opasnyh ob"ektov [The use of cryptographic protection of information in communication networks of physical protection systems of nuclear dangerous facilities]. *Svjaz' i avtomatizacija MVD Rossii*, 2004, pp. 48-51 (in Russian).

9. Braude-Zolotarev Ju. V., Maksimov S. A., Rudnev A. N., Sokolov E. E. Zashita kanalov tehniceskikh sredstv ohrany [Protection of Technical Security Channels]. *Sistemy Bezopasnosti*, 2002, no. 5, pp. 64-66 (in Russian).

10. Davydov Ju. L. Imitostojkie radiokanal'y tehniceskikh sredstv ohrany [Imitation Resistant Radio Channels of Technical Security Equipment]. *Transportnaja bezopasnost' i tehnologii*, 2007, no. 4, p. 33 (in Russian).

11. Samoylenko D. V., Eremeev M. A., Finko O. A. A method of providing the integrity of information in the group of robotic engineering complexes based on crypt-code constructions. *Automatic Control and Computer Sciences*, 2017, vol. 51, pp. 965-971. doi: 10.3103/S0146411617080181.

12. Samoylenko D., Eremeev M., Finko O., Dichenko S. Protection of Information from Imitation on the Basis of Crypt-Code Structures. *Advances in Soft and Hard Computing. ACS 2018. Advances in Intelligent Systems and Computing. Springer. Cham*. 2019, vol. 889, pp. 317-331. doi: 10.1007/978-3-030-03314-9_28.

13. Globin Y. O., Finko O. A. The way of ensuring resistant to imitation transmission information via communication channels. *H&ES Research*, 2020, vol. 12, no. 2, Pp. 30-43. doi: 10.36724/2409-5419-2020-12-2-30-43. (in Russian).

14. Braude-Zolotarev Ju. V. Algoritm bezopasnosti radiokanalov [Radio channel security algorithm]. *Algoritm Bezopasnosti*, 2013, no. 1, pp. 64-66 (in Russian).
15. Vasilevskij V. V., Zav'jalov S. A. Sposob peredachi izveshhenij dlja sistem centralizovannoj radioohrany [Method for transmitting notifications for centralized radio security systems]. *Omskij Nauchnyj Vestnik*, 2010, no. 2, pp. 203-206 (in Russian).
16. Wang Y., Attebury G., Ramamurthy B. *A Survey of Security Issues in Wireless Sensor Networks*. IEEE Communications Surveys and Tutorials, 2006. pp. 2-23. doi: 10.1109/COMST.2006.315852.
17. Kibirige G., Sanga C. *Attacks in Wireless Sensor Networks*. Sensor Technology: Concepts, Methodologies, Tools and Applications, 2020, pp. 1215-1232. doi: 10.4018/978-1-7998-2454-1.ch058.
18. Bilal M., Kang S.-G. *An Authentication Protocol for Future Sensor Networks*. Sensors, 2017, pp. 1-29. doi:10.3390/s17050979.
19. Yoo S.-G., Park K.-Y., Kim J. *A Security-Performance-Balanced User Authentication Scheme for Wireless Sensor Networks*. International Journal of Distributed Sensor Networks, 2012, pp. 1-11. doi:10.1155/2012/382810.
20. Zhang J., Varadharajan V. *Wireless Sensor Network Key Management Survey and Taxonomy*. Journal of Network and Computer Applications, 2010, pp. 63-75. doi: 10.1016/j.jnca.2009.10.001.
21. Wang Y., Attebury G., Ramamurthy B. *A Survey of Security Issues in Wireless Sensor Networks*. IEEE Communications Surveys and Tutorials, 2006, pp. 2-23. doi: 10.1109/COMST.2006.315852.
22. Bilal M., Kang S.-G. *Time-Assisted Authentication Protocol*. International Journal of Communication Systems, 2017, pp. 27-33.
23. Kumar P., Gurtov A., Ylianttila M., Lee S.-G., Lee H.-G. *A Strong Authentication Scheme with User Privacy for Wireless Sensor Networks*. ETRI Journal, 2013, pp. 889-899. doi: 10.4218/etrij.13.0113.0103.
24. Choi Y., Lee Y., Won D. *Cryptanalysis on Symmetric Key Techniques Based Authentication Scheme for Wireless Sensor Networks*. Computer Science and Ubiquitous Computing, 2015, pp. 7-13.
25. Zhou Y., Fang Y. *Defend Against Topological Attacks in Sensor Networks*. IEEE Military Communications Conference, 2006, pp. 1-6. doi: 10.1109/MILCOM.2005.1605774.
26. Olenin Ju. A. *Osnovy sistem bezopasnosti ob"ektov* [Basics of Facility Security Systems]. Penza, Penzenskij Gosudarstvennyj Universitet Publ., 2002. 118 p (in Russian).
27. State Standard R 50922–2006. Information Security. Main Terms and Definitions. Moscow, Standartinform Publ., 2006. 8 p. (in Russian).
28. ISO/IEC 7498-1:1994. *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*. ISO/IEC JTC 1, 1996. 59 p.

29. Bank dannyh ugroz bezopasnosti informacii [Information Security Threats Databank]. *Oficial'nyj sajt FSTJeK Rossii* [Official site of FSTEC of Russia], 10 June 2020. Available at: <https://bdu.fstec.ru/threat> (accessed 10 June 2020) (in Russian).
30. State Standard R 34.13–2015. Cryptographic Information Security. Block Cipher Modes. Moscow, Standartinform Publ., 2015. 23 p. (in Russian).
31. Bashurov V. V., Filimonenkov V. O., Yaroslavtsev A. A., Churikov Yu. I. Problem of Territory Security. *Journal of nuclear materials management*. USA. Fall, 2004. pp. 31-32.
32. Makarenko S. I., Rjumshin K. Yu., Mihajlov R. L. Model' funkcionirovaniya ob"ekta seti svyazi v usloviyah ogranichennoj nadjozhnosti kanalov svyazi [Model of Functioning of Telecommunication Object in the Limited Reliability of Communication Channel Conditions]. *Information Systems and Technologies*, 2014, vol. 86, no. 6, pp. 139-147 (in Russia).
33. R 1323565.1.006–2017. Information Technology. Cryptographic Information Security. Pseudorandom Sequence Generation Mechanisms. Moscow, Standartinform Publ., 2017. 7 p. (in Russian).
34. MR 26.2.003–2014. Information Technology. Cryptographic Information Security. Pseudorandom Sequence Generation Mechanisms. Moscow, Technical Committee on Standardization Publ., 2014. 8 p. (in Russian).
35. Grekul V. I., Denishhenko G. N., Korovkina N. L. *Proektirovanie informacionnyh system* [Information Systems Design]. Moscow, Binom Publ., 2012, 299 p. (in Russian).
36. MR 26.2.002–2016. Information Technology. Cryptographic Information Security. Cryptographic Algorithms for Generating Information Encryption Keys and Authentication Vectors Intended for Realization in Hardware Trust Modules for Use in Mobile Radiotelephone Communication. Moscow, Technical Committee on Standardization Publ., 2016. 13 p. (in Russian).
37. Samoylenko D. V., Ereemeev M. A., Finko O. A., Dichenko S. A. Parallel linear generator of multivalued pseudorandom sequences with operation errors control. *SPIIRAS Proceedings*, 2018, vol. 59, no. 4, pp. 31-61. doi: 10.15622/sp.59.2. (in Russian).
38. Finko O., Samoylenko D., Dichenko S., Eliseev N. Parallel generator of q-valued pseudorandom sequences based on arithmetic polynomials. *Przeglad Elektrotechniczny*, 2015, vol. 3, no 91, pp. 24-27. doi: 10.15199/48.2015.03.06.
39. Finko O., Dichenko S. Secure Pseudo-Random Linear Binary Sequences Generators Based on Arithmetic Polynoms. *Soft Computing in Computer and Information Science*, 2015, vol. 342, pp. 279-290. doi: 10.1007/978-3-319-15147-2_24.
40. Ventcel' E. S. *Teoriya veroyatnostej* [Probability Theory]. Moscow, Academy Publ, 2003. 576 p. (in Russian).
41. Gmurman V. E. *Teoriya veroyatnostej i matematicheskaja statistika* [Theory of Probability and Mathematical Statistics]. Moscow, Jurajt Publ, 2013. 479 p. (in Russian).
42. Verzhbickij V. M. *Osnovy chislennykh metodov* [Fundamentals of Numerical Methods]. Moscow, Vysshaya Shkola Publ, 2002. 840 p. (in Russian).

43. Kolmogorov A. N., Zhurbenko I. G., Prohorov A. N. *Vvedenie v teoriyu veroyatnostej* [Introduction to Probability Theory]. Moscow, Science Publ, 1982. 160 p. (in Russian).

Статья поступила 25 июня 2020 г.

Информация об авторах

Орлов Андрей Васильевич – соискатель ученой степени кандидата технических наук. Адъюнкт специальной кафедры. Краснодарское высшее военное училище имени генерала армии С.М. Штеменко. Область научных интересов: информационная безопасность; автоматизированные системы охраны; криптографические методы защиты информации. E-mail: aorlov-nauka@yandex.ru

Адрес: 350063, Россия, г. Краснодар, ул. Красина, д. 3.

Мельников Евгений Викторович – директор по информационным технологиям и защите информации АО «Тандер». Область научных интересов: безопасность информационных технологий в предпринимательской деятельности и бизнесе. E-mail: melnikov@magnit.ru

Адрес: 350072, Россия, г. Краснодар, ул. Солнечная, д. 15/5.

Финько Олег Анатольевич – доктор технических наук, профессор. Академический советник. Российская академия ракетных и артиллерийских наук. Профессор специальной кафедры. Краснодарское высшее военное училище имени генерала армии С. М. Штеменко. Область научных интересов: информационная безопасность и параллельные вычисления в алгебраических структурах; функциональный контроль и обеспечение отказоустойчивости средств обработки информации; контроль целостности и имитозащита данных. E-mail: ofinko@yandex.ru

Адрес: 350063, Россия, г. Краснодар, ул. Красина, д. 3.

Imitation Protection of Wireless Automated Security Systems for Sensitive Objects

A. V. Orlov, E. V. Melnikov, O. A. Finko

Purpose. High popularity for protection of the sensitive sites of different function, especially mobile type, with strict requirements to the speed of their reduction in a necessary ready state, was received by the wireless automated security systems (ASS) based on use of radio networks with cellular topology (so-called mesh-networks, wireless sensor networks and so forth). The main advantages of such systems of protection is the high speed of expansion/turning that is especially important for protection of objects of mobile type. Other important advantage of ASS – simplicity of scalability at protection of objects of various area and a configuration, and also at their modernization. Functioning of these systems on the basis of use of a radio channel for transfer of office messages staticizes questions of safety of transmitted data from imitating influences of the potential opponent. The known way of providing imitation protection of data based on development of message authentication code can lead to increase of probability of a compromise of key information at increase in number of security announcers and, therefore, to ASS exit from a condition of necessary level of security. **The aim of the work** is increase in level of immunity of the data transferred on ASS sensitive sites radio channels. Data protection algorithms from imitating influences of the opponent at various stages of functioning of system of protection, and also the technique of providing imitation protection of data consid-

ering features of construction and functioning of ASS sensitive sites in protected mode are offered. **Methods used:** theories of algorithms and the formalized description of cryptographic protocols; elements of the theory of casual processes (at estimation of security system of protection). **Novelty** of the offered algorithms and technique consists in new rules and receptions integration of the known cryptographic algorithms and protocols, and also their various modes of functioning providing protection of radio channels of ASS sensitive sites against various types of the imitating influences of the malefactor. **Results:** the complex of the algorithms of data protection transferred between elements of system of protection from imitating influences of the malefactor, allowing to exercise control of data on each of stages of their passing between system elements; the technique of providing an imitation protection of data including a number of the scientific and technical offers aimed at providing security of data from imitating influences of the opponent. Estimation of security system of protection is executed. **Practical relevance.** The received results allow to create ASS sensitive sites having a possibility of safe functioning in the conditions of imitating impacts by the opponent on it. At the same time the offered protocols are based on the cryptographic algorithms existing and standardized in the Russian Federation.

Key words: the automated system of protection, wireless sensor networks, message authentication code, imitation protection of data, radio channel immunity, cryptographic algorithms and protocols, protection of sensitive objects, a hash function, the digital signature, mesh-networks.

Information about Authors

Andrej Vasil'evich Orlov – postgraduate student of special Department. Krasnodar higher military school named after general of army S. M. Shtemenko. Field of research: information security, automated security systems, cryptographic methods of information security. E-mail: aorlov-nauka@yandex.ru

Address: Russia, 350063, Krasnodar, Krasina street, 4.

Evgeny Viktorovich Melnikov – director for information technologies and information protection of Tander JSC. Field of research: information technology security in entrepreneurship and business. E-mail: melnikov@magnit.ru

Address: Russia, 350072, Krasnodar, Solar street, 15/5.

Oleg Anatolyevich Finko – doctor of engineering, professor. Academic Advisor. Russian Academy of Rocket and Artillery Sciences. Field of research: information security and parallel computing in algebraic structures, functional control and fault tolerance of information processing, integrity control and data protection. E-mail: ofinko@yandex.ru

Address: Russia, 350063, Krasnodar, Krasina street, 4.