

$$P(R_{v,s,l}) = \begin{bmatrix} P(R_v) \\ P(R_s) \\ P(R_l) \end{bmatrix}. \quad (5)$$

Елементи матриці (5) будуть визначатися з виразів (2), (3), (4).

Враховуючи припущення, що події R_v , R_s , R_l незалежні і несумісні, ймовірність реалізації загрози захисту інформації в АСУ ТП можна представити у вигляді:

$$P(R) = \sum_{v=1}^V P(R_v) + \sum_{s=1}^S P(R_s) + \sum_{l=1}^L P(R_l). \quad (6)$$

Очевидно, що захист інформації буде забезпечено у випадку, якщо:

$$P(R) = 0. \quad (7)$$

III Висновки

Враховуючи викладене можна сформулювати наступні висновки:

- загрози і відповідно й механізми захисту АСУ ТП і звичайних автоматизованих систем відрізняються;
- значний вплив на інформаційну безпеку ОКІ має соціокультурний аспект;
- для розробки адекватних рекомендацій, методів та засобів щодо захисту інформації в АСУ ТП можливо застосовувати запропоновану загальну модель загроз захисту інформації АСУ ТП;
- при здійсненні розрахунку ймовірності реалізації загроз від атак на технічний компонент необхідно враховувати дію дестабілізуючих впливів на соціокультурний компонент.

Список використаної літератури: 1. Васильев Ю. К. Анализ международного досвіду щодо визначення ключових систем інформаційної інфраструктури / Васильев Ю. К. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2014. – Вип. 1(27). – С. 43-47. 2. Леоненко Г. П., Юдин А. Ю. Проблемы обеспечения информационной безопасности систем критически важной информационной инфраструктуры Украины // Information Technology and Security. -2013. – Вип. 1(3). - С. 44. 3. Гончар С. Ф. Методологічні засади розробки та впровадження систем захисту інформації на об'єктах критичної інфраструктури / Гончар С. Ф., Леоненко Г. П., Юдин О. Ю. // Спеціальні телекомунікаційні системи та захист інформації. – 2014. - Вип. 1(25). – С. 158-163. 4. Гончар С. Ф. Анализ угроз и уязвимостей промышленных автоматизированных систем управления / Гончар С. Ф., Леоненко Г. П., Юдин А. Ю. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2013. – Вип. 2(26). – С. 9-14. 5. Анализ угроз сетевой безопасности [Электронный ресурс]. – Режим доступа: <http://ypn.ru/138/analysis-of-threats-to-network-security/6/>. 6. Лукацкий Алексей. Статистика реальных инцидентов ИБ в промышленных системах [Электронный ресурс]. – Режим доступа: http://www.securitylab.ru/blog/personal/Business_without_danger/38672.php. 7. Гончар С. Ф., Леоненко Г. П., Юдин О. Ю. Соціокультурний аспект забезпечення інформаційної безпеки об'єктів критичної інфраструктури : тези доповідей XX Всеукраїнської науково-практичної конференції «Проблеми створення, розвитку та застосування високотехнологічних систем спеціального призначення», Житомир, – 2014. - С. 195-196. 8. Ловцов Д. А., Сергеев Н. А. Управление безопасностью эргосистем / Под ред.. Д. А. Ловцова, - 2-е изд. испр. и доп. – М.: РАУ-Университет, 2001. - 224 с.

Елена Азаренко, Олег Бляшенко, Михаил Дивизинюк, Валерия Ковач

Государственное учреждение «Институт геохимии окружающей среды НАН Украины»

УДК 504.455.064.3:574 (262.5)

ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМАХ МОНИТОРИНГА ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ

Аннотация: Показано, что системы мониторинга чрезвычайных ситуаций являются гибридными системами с аналого-цифровой обработкой передаваемой информации. Защита информации, циркулирующей в ней, должна основываться на наличии в ее составе трех типов подсистем, каждая из которых должна отвечать своим специфическим требованиям.

Summary: In the article it is shown that the emergency monitoring systems are hybrid systems with analogue-digital processing of the data conversion. Protection of information circulating in it should be based on the presence in its composition of three types of subsystems, each of which must meet their specific requirements.

Ключевые слова: Гибридные системы, аналого-цифровое преобразование информации, системы мониторинга, декомпозиция, погрешность.

I Введение

Системы мониторинга чрезвычайных ситуаций служат эффективным средством предупреждения и предотвращения аварий и катастроф. Они позволяют своевременно обнаружить негативные факторы и не допустить их развития. Одним из видов таких систем являются системы мониторинга морских захоронений боевых отравляющих веществ [1 – 3].

Сейчас в районах морских захоронений боевых отравляющих веществ возникают две проблемы. Первая экологическая. Металлические бочки корродируют, нарушается их герметичность, и иприт попадает в водную среду, переносится потоком придонных вод, уничтожая все живое на своем пути [4]. Вторая – террористическая. Различные коммерческие организации готовы поднимать сохранившиеся емкости с морского дна с целью перепродажи их третьим лицам, а экстремисты различной направленности могут использовать их для проведения террористических актов в местах массового скопления людей или политического шантажа населения и правительства [5].

Системы подводного мониторинга сигнализируют о нарушении герметичности бочек и выходе иприта наружу, а также о целостности всего морского захоронения [6]. Передаваемая телеметрическая информация должна быть защищена, чтобы своевременно обнаружить утечку иприта и принять меры к его нейтрализации, не допустив паники среди населения прибрежных районов [7 – 8]. Разработка комплекса организационно-технических мероприятий по защите информации, циркулирующей в подобных системах мониторинга, должна быть соответствующим образом спроектирована [9] и удовлетворять всем требованиям по управлению информационной безопасностью [10].

II Постановка цели и задачи статьи

Целью данной работы является определение методологических подходов к разработке комплекса мероприятий по защите телеметрической информации, передаваемой в системах мониторинга чрезвычайных ситуаций, на примере морских захоронений боевых отравляющих веществ.

Для достижения поставленной цели необходимо решить следующие задачи. Во-первых, рассмотреть основные элементы системы мониторинга чрезвычайных ситуаций и требования к передаваемой телеметрической информации. Во-вторых, определить основные подходы к защите телеметрической информации.

III Основные элементы системы мониторинга и структура передаваемой телеметрической информации

Основу системы мониторинга составляет измерительный элемент. Измерительный элемент посредством кабель-троса крепится к якорю, а вторая его часть к радиобуй или к поплавку, который обеспечивает его размещение на заданном удалении от морского дна. Радиобуй может быть на одном центральном элементе. Здесь же могут располагаться элементы электропитания (аккумуляторы, солнечные элементы, ветрогенераторы), которые обеспечивают работу всех элементов системы.

В состав измерительного элемента системы мониторинга входят прямой и косвенный измерители скорости звука.

В измерительную базу прямого измерителя скорости звука входят излучатель и приемник, выполненные из пьезоэлектрического материала и жестко закрепленные на измерительной базе. Микропроцессор первого уровня, входящий в состав прямого измерителя, управляет его работой. Управляющий сигнал от микропроцессора поступает на цифроаналоговый преобразователь, который в свою очередь, запускает генератор. Сформированный генератором электрический сигнал излучается в водное пространство в виде акустической волны и, пройдя измерительную базу, принимается приемником. Здесь не является принципиальным, какой сигнал излучается. Он главным образом определяется типом и конструкцией прямого измерителя скорости звука. Лабораторные эксперименты показали, что и импульсные и фазовые прямые измерители скорости звука одинаково реагируют на наличие антропогенных примесей. Принятый приемником акустический сигнал усиливается и после преобразования аналого-цифровым преобразователем поступает в микропроцессор первого уровня. Микропроцессор проводит необходимые вычисления и значение скорости звука, измеренное прямым измерителем, поступает в управляющий микропроцессор.

В косвенном измерителе три канала: температуры, электропроводности и гидроакустического давления. Каждый из этих датчиков подключается в одно из плеч измерительного моста. Результирующий аналоговый сигнал поступает в аналого-цифровой преобразователь, а затем на микропроцессор первого уровня. Вычисленные значения температуры, электропроводности (солености) и гидроакустического давления поступают на управляющий микропроцессор, где происходит окончательное вычисление скорости звука, измеренное косвенным измерителем, и его последующие сравнение со значением скорости звука, полученное прямым измерителем.

Помимо выше описанных функций управляющий микропроцессор синхронизирует измерения, и обеспечивает трансляцию телеметрической информации на главный пост системы мониторинга.

С главного поста на элементы системы мониторинга передаются управляющие сигналы. С элементов на главный пост передача осуществляется в стандартном, экономичном и экстремальном режимах. В стандартном режиме передаются данные об измерениях скорости звука – параметра обеспечивающего обнаружение иприта и состояние каждого элемента, свидетельствующее о целостности захоронения. Эти данные могут транслироваться с интервалом 15, 30 и 60 минут. В экономном режиме режим передачи данных увеличивается до 2, 4 и 8 часов. В экстремальном режиме, наоборот, интервал сокращается до 10, 5 и 2 минут.

IV Основные подходы к защите информации, передаваемой в системах мониторинга

Будем рассматривать совокупность всех элементов системы мониторинга, каналы передачи информации, как гибридную систему, в которой циркулирует определенная информация (совокупность аналоговых и цифровых сигналов). Тогда требования, определяющие защиту информации, будут соответствовать решению задачи декомпозиции или определения компонентов вектора внешних параметров структурных элементов. К векторным внешним параметрам относятся такие компоненты, как характеристики инструментальной погрешности при измерениях, квантование сигнала по уровням, спектральная характеристика помех и т. д. В то же время каждая из этих составляющих может раскладываться на составные специфические параметры.

Формулируя требования к компонентам векторных параметров, решается два вопроса. Первый – какие компоненты являются существенными при использовании в данной системе (семантическая декомпозиция). Второй – какие ограничения должны быть наложены на существенные компоненты (количественная декомпозиция). Выполнение семантической декомпозиции позволяет конкретизировать условия функционирования гибридной системы в целом. Количественная декомпозиция является дальнейшим шагом на пути конкретизации мероприятий защиты. Она производится только для существенных компонент, то есть по результатам семантической декомпозиции.

Рассмотрим семантическую декомпозицию на примере результирующей погрешности для гибридных систем трех типов.

Системы первого типа, в которых преобразование информации должно быть инвариантным с требуемой точностью только к математическим ожиданиям и корреляционным функциям преобразуемых и передаваемых сигналов.

Поскольку аналогово-цифровые преобразования являются одним из этапов обработки информации и всегда вносит погрешность, представляет интерес поиск условий инвариантности, при которых отсутствует влияние этой погрешности на точность характеристик, вычисляемых по результатам преобразования. Другими словами задача состоит в том, чтобы найти требования к отдельным погрешностям аналогово-цифрового преобразования, при которых не равная нулю результирующая погрешность не влияет на точность системы в целом. Такие требования могут быть установлены следующим образом.

Рассмотрим аналогово-цифровое преобразование как идеальный импульсный элемент, на входе которого действует аддитивная смесь преобразуемого сигнала $X(t)$ и погрешности $P(t)$ (неаддитивные составляющие погрешности).

Импульсный элемент осуществляет временную дискретизацию входного сигнала с некоторым постоянным шагом T . Тогда сигнал на выходе рассматриваемой модели представляет собой случайную последовательность $Y_i = X_i + P_i$ ($i=1,2,\dots$).

Запишем выражение для математического ожидания $M_y(i)$ и автокорреляционной функции $K_y(i,j)$ последовательности Y_i

$$M_y(i) = E(X_i) + E(P_i), \quad (1)$$

$$\begin{aligned} K_y(i,j) &= E((X_i + P_i - M_y(i)) (X_j + P_j - M_y(j))) = \\ &= E(X_i X_j) + E(X_i P_j) - E(X_i M_y(j)) + E(X_j P_i) + E(P_i P_j) - \\ &- E(P_i M_y(j)) - E(X_j M_y(i)) - E(P_j M_y(i)) + E(M_y(i) M_y(j)), \end{aligned} \quad (2)$$

где E – символы операции математического ожидания, $j = 1, 2, \dots$

Условия инвариантности аналогово-цифрового преобразования относительно математического ожидания $M_x(i)$ и автокорреляционной функции $K_x(i, j)$ сигнала X_i можно записать в виде

$$M_x(i) = M_y(i), \quad (3)$$

$$K_x(i, j) = E(X_i X_j) - M_x(i) M_x(j) = K_y(i, j). \quad (4)$$

Анализ (1) и (2) показывают, что (3) и (4) имеют место, если

$$E(\Pi_i) = 0, \quad (5)$$

$$E(X_i \Pi_j) = E(X_j \Pi_i) = 0, \quad (6)$$

$$E(\Pi_i \Pi_j) = 0. \quad (7)$$

Для выполнения (6) и (7) при условии (5) необходимо и достаточно, чтобы элементы последовательности Π_i были не коррелированы с элементами последовательности X_i и между собой (внутренняя некоррелированность).

При $i=j$ равенство (7) не выполняется, так как мощность погрешности при аналогово-цифровых преобразованиях не равна нулю. Более того, при вычислении автокорреляционной функции в точке (i, i) по форме (2) условия (5), (6), (7) не является достаточным для обеспечения инвариантности относительно дисперсии $K_x(i, i) = D_x(i)$. Поэтому введем дополнительные ограничения на погрешность Π_i .

Необходимо, чтобы последовательность Π_i была стационарной относительно дисперсии $D_{\Pi}(i)$, то есть $D_{\Pi}(i) = D_{\Pi} = \text{const}$. Тогда, если величина D_{Π} известна, смещенность оценки $D_y(i)$ для дисперсии $D_x(i)$, можно устранить в соответствии с формулой

$$D_x(i) = D_y(i) - D_{\Pi} \quad (8)$$

Таким образом, условия инвариантности аналогово-цифровых преобразований сводятся к четырем требованиям в отношении погрешности, а именно: равенства нулю математического ожидания, некоррелированности с преобразуемым сигналом, внутренней некоррелированности и стационарности по дисперсии.

Системы второго типа, в которых преобразование информации должно обеспечить требуемую скорость передачи информации или пропускную способность. Если такая схема включает в себя аналогово-цифровое преобразование, то при ее оптимизации необходимо определить, как отдельные составляющие результирующей погрешности влияют на скорость передачи информации и пропускную способность.

Рассмотрим идеальный импульсный элемент, на входе которого аддитивная смесь сигнала $X(t)$, высокочастотной погрешности $B(t)$ и низкочастотной погрешности $\Gamma(t)$, то есть

$$Y_i = X_i + B_i + \Gamma_i, \quad \text{где } (i=1, 2, \dots). \quad (9)$$

Элементы последовательности B_i в силу высокочастотных свойств погрешности статистически взаимно независимы. Поскольку погрешность $\Gamma(t)$ низкочастотная, ее элементы сильно коррелированы. Поэтому выполняется следующие соотношения

$$\sigma(B_s) = \sigma(B_s | \zeta_{s-1}, \zeta_{s-2}, \dots, \zeta_{s-m_{\zeta+1}}), \quad (10)$$

$$\sigma(\Gamma_s) \gg \sigma(\Gamma_s | \gamma_{s-1}, \gamma_{s-2}, \dots, \gamma_{s-m_{\gamma+1}}). \quad (11)$$

На взаимную корреляцию элементов последовательности X_i , а также функцию плотности вероятности и стационарность процессов $X(t)$, $B(t)$ $\Gamma(t)$, не налагаем никаких ограничений.

В соответствии с теорией Шеннона скорость передачи информации R на момент времени sT имеет вид

$$R_s = \frac{1}{T} (H_s(Y) - H_s(\Pi)), \quad (12)$$

где $H_s(Y)$ – энтропия текущего S элемента последовательности Y ; $H_s(\Pi)$ – энтропия текущего S элемента последовательности $\Pi_i = B_i + \Gamma_i$

Обобщая представление энтропии в форме Новицкого и предлагая, что без существенного ограничения общности $\sigma(B_s) \geq \sigma(\Gamma_s)$ и выполнив не сложные преобразования получим значение скорости передачи информации

$$R_s \approx \frac{1}{T} (E_{\Pi, X} (\log(2K(N_s | n_{s-1}, n_{s-2}, \dots, n_{s-m_{n+1}})) \times \\ \times (\sigma^2(X_s | X_{s-1}, X_{s-2}, \dots, X_{s-m_{n+1}}) + \sigma(B_s))^{\frac{1}{2}} - \\ - \log(2K(B_s)\sigma(B_s))) = \frac{1}{T} (H_s(N) - H_s(B)) \quad (13)$$

где $N_i = X_i + B_i$; $H_s(N)$ – энтропия S элемента последовательности N ; $H_s(B)$ – энтропия S элемента последовательности B .

Таким образом, влияние низкочастотной погрешности на скорость передачи информации при аналогово-цифровом преобразовании незначительна и ею можно пренебречь.

Системы третьего типа, в которых аналогово-цифровое преобразование должно быть инвариантным с требуемой точностью по отношению ко всем характеристикам преобразуемых и передаваемых сигналов. Другими словами, необходимо с требуемой точностью передать весь ход преобразуемого и передаваемого процесса $X(t)$.

Пусть составляющие результирующей погрешности статистически взаимно независимы и характеризуются среднеквадратическими значениями σ_i ($i=1, \dots, n$). Тогда решение задачи декомпозиции будет определяться из следующего соотношения

$$D_t = F_t \left(\log \frac{12\sigma^4}{2 \sum_{j=1}^{n-1} \sigma_j^2 + \sigma_n^2} + \sqrt{\frac{\sum_{j=1}^{n-1} \sigma_j^2}{\sigma^2}} \log 2,846 \right), \quad (14)$$

где F_t – максимальная частотная составляющая в спектре преобразуемого и передаваемого сигнала; σ – среднеквадратическое значение результирующей погрешности; σ_n – среднеквадратическое значение погрешности квантования сигнала по уровням.

Критерий D_t может принимать различные значения в зависимости от состояния между величинами σ и σ_n . Максимальное значение соответствует варианту аналогово-цифрового преобразования с худшим сочетанием составляющих погрешности, а минимальное – наилучшему.

Таким образом, при заданных параметрах среднеквадратичных значений результирующей погрешности, необходимо чтобы соотношения между погрешностью квантования и остальными ее составляющими было существенно меньше единицы.

В Выводы

Система мониторинга чрезвычайных ситуаций, на примере система мониторинга морских захоронений боевых отравляющих веществ, является гибридной системой с аналого-цифровой обработкой передаваемой информации. Разработка мероприятий по защите информации, циркулирующей в системе, должно основываться на наличии в ее составе структурных подсистем трех типов, каждой из которых ставятся конкретные требования. Системам первого типа – инвариантное преобразование информации, второго типа – обеспечение требуемой скорости передачи информации, третьего – быть инвариантными с требуемой точностью ко всем характеристикам преобразуемых и передаваемых сигналов.

Список использованных источников: 1. Азаренко Е. В. Проблема управления экологической безопасностью прибрежных вод и пути ее решения/ Е. В. Азаренко, Ю. Ю. Гончаренко, М. М. Дивизинюк // Збірник наукових

праць «Системи обробки інформації». – Харків: ХУПС ім. Івана Кожедуба, 2012. – Вип.2 (100). – С. 271 – 275. 2. Азаренко Е. В. Компьютерный эколого – экономический мониторинг как информационно – техническое средство управления экологической безопасностью / Е. В. Азаренко, Ю. Ю. Гончаренко, М. М. Дивизинюк // *Наук.-техн. журнал «Сучасний захист інформації»*. – Київ: ДУІКТ, 2012. – Спецвипуск. – С. 53 – 56. 3. Гончаренко Ю.Ю. Иприт и особенности его трансформации // *Сб. науч. тр. МГИ НАН Украины «Системы контроля окружающей среды»*. – Севастополь: МГИ, 2012. – Выпуск 18. – С. 25-29. 4. Азаренко Е. В. Закономерности трансформации иприта в эмульгированное состояние / Е. В. Азаренко, Ю. Ю. Столярчук // *Збірник наукових праць «Системи озброєння та військова техніка»*. – Харків: ХУПС ім. Івана Кожедуба, 2014. – Вип.4 (40). – С. 147-150. 5. Азаренко Е. В. Факторы определяющие экологическую обстановку в районе свала морских глубин северо – западной части Черного моря / Е. В. Азаренко, С. А. Чернявская, Ю. Ю. Гончаренко, // *Збірник наукових праць СНУЯЕтаП*. – Севастополь: СНУЯЕтаП, 2013. – Вип. 3 (47). – С. 202 – 208. 6. Азаренко Е. В. Система мониторинга чрезвычайных ситуаций в районах морских захоронений боевых отравляющих веществ/ Е. В. Азаренко, О. В. Бляшенко, М. М. Дивизинюк, В. Е. Ковач// *Збірник наукових праць «Моделирование та інформаційні технології»*. – Київ: Інститут проблем моделювання в енергетиці ім. Г.С. Пухова, 2014. – Вип. 73. – С. 79 – 86. 7. Азаренко Е. В. Компьютерный эколого – экономический мониторинг как информационно – техническое средство управления экологической безопасностью/ *Наук.-технич. Журнал «Сучасний захист інформації»*. – Київ: ДУІКТ, 2012. – Спецвипуск. – С. 53 – 56. 8. Дивизинюк М. М. Классификация чрезвычайных ситуаций социального характера/ М. М. Дивизинюк, О. В. Бляшенко, Т. В. Ковалюк// *Збірник наукових праць СНУЯЕтаП*. – Севастополь: СНУЯЕтаП, 2012.- Вип. 2(42). – С. 217 – 220. 9. Хорошко В. А. Проектирование систем технической защиты информации /В. А. Хорошко, М. М. Дивизинюк, Ю. Ю. Гончаренко и др. Учеб. пособие. – Севастополь: СНУЯЭиП, 2011. – 235 с. 10. Хорошко В. О. Методи керування інформаційною безпекою / В. О Хорошко, М. М. Дивізінюк, Ю. Ю. Гончаренко та інші. Навч. Посібник. – Севастополь: СНУЯЕтаП, 2010. – 328 с.

Андрій Паламарчук, Дмитро Вергелес, Володимир Гуменюк, Юрій Васильєв, Олег Белас*, Олег Іванько*, Сергій Мазор*

*ДержНДІ Спецзв'язку, *ІСЗЗІ НТУУ "КПІ"*

УДК 638.235.231

ДОСЛІДЖЕННЯ ЕЛЕМЕНТА АНТЕННОЇ РЕШІТКИ ЯК ОПРОМІНЮВАЧА ПАРАБОЛІЧНОЇ АНТЕНИ ДЛЯ СТАНЦІЙ ТРОПОСФЕРНОГО ЗВ'ЯЗКУ

Анотація: Наведено дослідження антенної решітки, що є опромінювачем параболічної антени діапазону 4,5...4,7 ГГц. Симетричний вібратор (СВ) горизонтально розміщений над екраном, створює при довжині плеча $0,75\lambda$ "нерозвалену" діаграму направленості з провалом в центрі, що дозволяє підвищити коефіцієнт використання поверхні. В статті, також, показаний вигравш в підсиленні при використанні двох паралельних СВ.

Summary: Questions investigation array that is irradiator parabolic antenna range 4.5 ... 4,7GHz. Symmetric vibrator (SV) horizontally placed above the screen makes at shoulder length $0,75\lambda$ "not-disorganized" chart orientation of failure in the center, which improves utilization of surface. The paper also shows a gain in strengthening using two parallel SV.

Ключові слова: Опромінювач, антена решітка, симетричний вібратор, діаграма направленості, коефіцієнт підсилення, коефіцієнт направленої дії, власний опір, наведений опір.

І Вступ

Антенна станції тропосферного зв'язку є однією із найбільш складних частин апаратури. Внаслідок великого ослаблення поля при тропосферному поширенню радіохвиль та виникнення спотворень сигналів необхідно забезпечувати значну ефективну ізотропну випромінювану потужність (ЕІВП). Це можливо забезпечити шляхом збільшення коефіцієнта підсилення антени (G) та потужності передавача.

Для отримання необхідної ЕІВП, розглянуто можливість використання параболічної антени та розроблення багатоелементного опромінювача, який представляє собою решітку з двох груп лінійних симетричних вібраторів – опромінювачів. Антена з такими опромінювачами та певною кількістю малопотужних підсилювачів може забезпечити необхідну ЕІВП.