СИСТЕМА БЕЗАВАРИЙНОГО УПРАВЛЕНИЯ КРИТИЧЕСКИ ВАЖНЫМИ ОБЪЕКТАМИ В УСЛОВИЯХ КИБЕРНЕТИЧЕСКИХ АТАК

Жиленков А.А.[1], Черный С.Г.[2]

Целью исследования *является разработка ряда подходов для количественной оценки кибербезопасности сетевых систем управления и обнаружения кибернетических атак на данные системы.*

Метод исследования: *исследуемая система описывается моделью дискретного пространства-времени с время-инвариантной обратной связью, детектирование атак в которой осуществляется посредством предложенного детектирующего фильтра. Анализируются возможные цели и ресурсные ограничения злоумышленника в целевой системе управления, результаты воздействия атак на неё, предлагается метод обнаружения атаки. Осуществлен анализ компонентных и кроссплатформенных структур. Сделаны выводы о структурах совмещения и коллизии.*

Результат исследования: *на основе предложенных оценок максимальной интенсивности возможного воздействия, а также достаточных и необходимых ресурсов для его реализации, предложен алгоритм обнаружения кибернетической атаки на сетевую систему управления. Подход обладает рядом преимуществ его реализации, одно из которых экономичность внедрения. Работоспособность предложенного подхода проиллюстрирована на примере управления критически важным объектом морского транспорта. Разработанные практические примеры являются актуальными и реализованы на практике на паромах, действующих на Керченской паромной переправе. Реализованная модель позволяет обеспечить защиту от кибернетических атак на балластную систему критически важного объекта морского транспорта.*

Ключевые слова: *морской транспорт, кибербезопасность, система управления, балласт, ограничения, отказоустойчивость, детектирование атак.*

DOI:10.21681/2311-3456-2020-2-58-66

Актуальность

Возрастающая сложность автоматизированных систем управления (АСУ), переход к цифровым системам и стремление к объединению их в интегрированные комплексы управления объектами и технологическими процессами (ТП) привели к развитию и внедрению гетерогенных систем, совмещающих дискретные и непрерывные подсистемы с передачей данных по цифровым линиям связи. Сегодня данные системы могут обмениваться информацией не только в локальных сетях предприятия, но и, как правило, имеют доступ к глобальной сети интернет, что позволяет следить за их функционированием и производить при необходимости коррекцию работы, обновление программного обеспечения и т.п., без вывода их из эксплуатации. Анализ [1-2] показывает, что данные возможности заложены в том числе в большинстве АСУ ТП критически важных объектов (КВО). Например, буровые установки морского базирования, эксплуатируемые в азово-черноморском бассейне, оборудованы АСУ ТП зарубежного производства, в которых реализована возможность удалённого мониторинга и управления посредством системы спутниковой связи фирмой-производителем даже без ведома предприятия, эксплуатирующего данную установку. Очевидно, что помимо собственника и производителя оборудования удалённый доступ к нему могут получить и несанкционированные лица, в связи с чем остро встаёт проблема обеспечения кибернетической безопасности АСУ ТП КВО.

За последние годы количество кибернетических угроз для подобных объектов увеличилось значительно и продолжает расти, что объяснимо, учитывая большое количество возможных точек для атаки на различных уровнях систем. На сегодняшний день широкую огласку получили множество случаев кибератак, таких как атака на электроэнергетическую систему [3], недавняя атака компьютерного вируса на систему управления предприятия [4, 5] и т.п. Мониторинг и предотвращение кибератак имеют решающее значение, поскольку они могут привести к катастрофическим последствиям, что наглядно демонстрирует пример последствий американо-канадского обесточивания энергосистем 2003 года [6].

1 Жиленков Антон Александрович, доцент, кандидат технических наук, заведующий кафедрой морской электроники Санкт-Петербургского государственного морского технического университета. IEEE member, DAAAM, Санкт-Петербург, Россия. E-mail: zhilenkovanton@gmail.com

2 Черный Сергей Григорьевич, кандидат технических наук, доцент кафедры «Электрооборудование судов и автоматизации производства» Керченского государственного морского технологического университета, доцент ГУМРФ имени С.О. Макарова. IEEE member, DAAAM, EAI. Керчь – Санкт-Петербург, Россия. E-mail: sergiiblack@gmail.com

Особо сложной в плане выявления кибератакой является удалённое введение злоумышленником ложных данных, подменяющих действительные данные, передаваемые по каналам управления или обратных связей [7-9]. В настоящей статье рассмотрены именно подобные сценарии кибератак, использующих ложные данные, генерируемые таким образом, чтобы, как предполагается злоумышленником, они не были обнаружены в потоке данных управляющего ввода и измерения, а также предлагаются детекторы отклонений для их выявления и предотвращения кибератак.

Существующие решения

В [10] авторами анализируется набор стратегий скрытых атак, использующих ложные данные, в случае когда злоумышленники имеют доступ к информации о точной модели объекта и полный доступ к сигналам всех датчиков и исполнительных каналов системы. В [11] анализируются атаки с введением скрытых ложных данных с допущением о злоумышленниках, обладающих полной информацией о состоянии системы, но имеющих доступ к искажению данных только некоторого подмножества датчиков и исполнительных механизмов. В [12] рассматривается конечный интервал времени кибератаки и оценивается число поврежденных каналов, которые не могут быть обнаружены в течение данного интервала времени.

Во всех приведённых примерах использованы допущения, что данные каналов управления и измерения, доступные для предлагаемого детектора отклонений, до атаки и во время нее были одинаковы и атака не была обнаружена. В настоящей статье рассматриваются более гибкие сценарии предотвращения атак, которые теоретически могут быть обнаружены, но скрыты, поскольку не вызывают срабатывания детекторов отклонений, приведённых в работах [10-14].

Предварительные сведения

Для дальнейших рассуждений будем использовать следующее описание сигналов дискретного времени.

Пусть $\{x_{k_0}, x_{k_0+1}, \ldots, x_{k_f}\}$ – выборки сигналов дискретного времени по $n \in \mathbb{Z}$ каналам во временном интервале $[k_0, k_f] = \{k_0, \ldots, k_f\}$, при $k \in [k_0, k_f]$. Для упрощения, представим совокупность выборок сигналов x_k на временном интервале $[k_0, k_f]$ в векторной форме как $\boldsymbol{x}_{[k_0,\, k_f]} \in \mathbb{R}^{n(k_f-k_0+1)}$, при $\boldsymbol{x}_{[k_0,\, k_f]} = \left[x_{k_0}^T, \ldots, x_{k_f}^T\right]^T$. Для известного временного интервала, вместо $\boldsymbol{x}_{[k_0,\, k_f]}$ будем использовать сокращённое обозначение $\boldsymbol{x}$.

Пусть l_p-норма дискретного сигнала $\boldsymbol{x}$ на интервале $[k_0, k_f]$, определяется как

$$\|x\|_{l_p[k_o,k_f]} \stackrel{\Delta}{=} \left\|x_{[k_0,k_f]}\right\|_p = \left(\sum_{k=k_0}^{k_f} \|x_k\|_p^p\right)^{\frac{1}{p}},$$

при $1 \le p < \infty$,

и пусть $\|x\|_{l_\infty[k_o,\, k_f]} \stackrel{\Delta}{=} sup_{\;\; k\in[k_0,\, k_f]} \left\|x_f\right\|_\infty$.

Далее, для некоторого $y \in \mathbb{C}^n$ обозначим *p*-норму от *y*, как $\|y\|_p \stackrel{\Delta}{=} \left(\sum_{i=1}^n |y_{(i)}|^p\right)^{\frac{1}{p}}$, при $1 \le p < \infty$, где $y(i)$ – *i*-я составляющая вектора *y*.

Причём, $\|y\|_\infty \stackrel{\Delta}{=} max_{\;\; i}\, |y(i)|$, а $\|y\|_0$ – число ненулевых элементов y.

Пусть $\mathbb{S} = \{z \in \mathbb{C} : |z| = 1\}$ – единичная окружность на комплексной плоскости.

Пусть дана некоторая матрица $G \in \mathbb{C}^{n\times m}$. Будем обозначать как G^H её эрмитово сопряжённое, а $G^* = (G^H H)^{-1} G^H$ её псевдообратную матрицу.

Постановка задачи исследования

Рассмотрим типичную архитектуру сетевой системы управления некоторым объектом [1-2, 9-15], подвергающуюся атаке с вводом ложных данных.

Выделим в структуре рассматриваемой сетевой системы управления три основных компонента (рис. 1):

- физический объект управления и сеть передачи данных;
- контроллер обратной связи;
- детектор отклонений.

Физический объект управления (ОУ) опишем моделью дискретного пространства-времени (1):

$$P: \begin{cases} x_{k+1} = Ax_k + B\tilde{u}_k + G\omega k + Ff_k, \\ y_k = Cx_k + \upsilon_k, \end{cases} \quad (1)$$

где $x_k \in \mathbb{R}^n$ – переменная состояния; $\tilde{u}_k \in \mathbb{R}^{n_u}$ – управляющие воздействия; $y_k \in \mathbb{R}^{n_y}$ – показания датчиков в момент выборки $k \in \mathbb{Z}$; $f_k \in \mathbb{R}^d$ – неизвестный сигнал, описывающий эффекты отклонений (сигнал неисправности [3]); $w_k \in \mathbb{R}^n$ и $\upsilon_k \in \mathbb{R}^{n_y}$ –

гауссовский шум в каналах управления и измерений представляет собой расхождение между моделью и реальным процессом, возникающее из-за не моделируемых в явном виде возмущений. Будем полагать, что среднее для w_k и v_k ограничено значениями соответственно δ_w и δ_v, то есть $\overline{w} = \|E\{w_k\}\| \le \delta_w$ и $\overline{v} = \|E\{v_k\}\| \le \delta_v$.

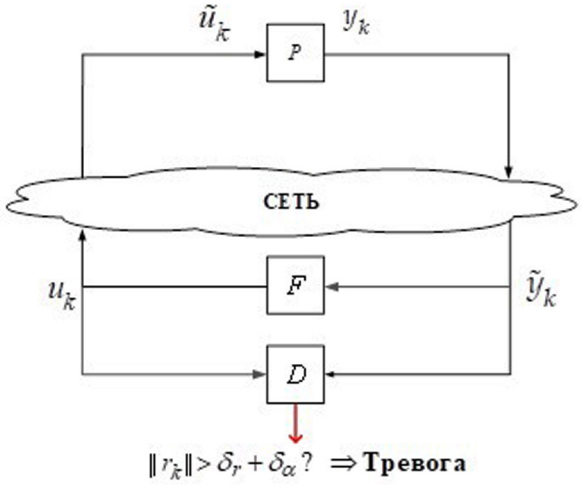

Рис. 1. Схема сетевой системы управления

Данные измерений датчиков y_k и управляющей информации исполнительных устройств $\tilde{u}_k$ передаются через информационную сеть. На стороне контроллера соответствующие сигналы обозначим как $\tilde{y}_k \in R^{n_y}$ и $u_k \in R^{n_u}$. В настоящей статье не рассматриваются такие характерные для сетей передачи данных эффекты, как потери пакетов данных и стохастические запаздывания, то есть сеть считаем идеальной и надёжной, не влияющей на данные, передаваемые через нее, что вполне справедливо для КВО морских объектов [15-17].

Учитывая физическую модель установки (1) и предположение о идеальной сети передачи данных, считаем, что сетевая система управления имеет номинальное поведение, если $f_k = 0, \tilde{u}_k = u_k, \tilde{y}_k = y_k$. Отсутствие одного из этих условий приводит к ошибочному поведению системы.

Чтобы обеспечить заданные показатели качества управления при наличии шумов в сигналах управления и данных измерений, считаем, что система автоматического управления охватывается время-инвариантной линейной обратной связью (ОС). Данный контроллер с ОС может быть описан как

$$F: \begin{cases} z_{k+1} = A_c z_k + B_c \tilde{y}_k, \\ u_k = C_c z_k + D_c \tilde{y}_k, \end{cases} \quad (2)$$

где параметры состояния контроллера $z_k \in R^{n_z}$ могут включать в себя состояние процесса управления и оценки ошибок.

Введём также описание детектора отклонений, предназначенного для обнаружения возможных отклонений от номинального поведения системы. Предполагается, что детектор отклонений совмещен с контроллером, поэтому он имеет доступ только к y_k и u_k для оценки поведения объекта управления.

В литературе, посвящённой диагностике неисправностей [3, 6], описывается несколько общепринятых подходов к обнаружению неисправностей в системах управления. Рассмотрим следующий фильтр обнаружения аномалий

$$D: \begin{cases} \hat{x}_{k+1|k} = A\hat{x}_{k|k} + Bu_k, \\ \hat{x}_{k|k} = \hat{x}_{k|k-1} + K(y - C\hat{x}_{k|k-1}), \\ r_k = V(\tilde{y}_k - y_{k|k}), \end{cases} \quad (3)$$

где $\tilde{x}_{k|k} \in R^n$ и $\tilde{y}_{k|k} = C\hat{x}_{k|k} \in R^{n_y}$ – оценки состояния и выхода дающие значения измерений до времени *k*, соответственно, а $r_k \in R^{n_r}$ – остаток, взвешенный для обнаружения и локализации существующих отклонений. Описанный фильтр может быть описан как

$$D: \begin{cases} \hat{x}_{k+1|k} = A(I - KC)\hat{x}_{k-1|k} + Bu_k + AK\tilde{y}_k, \\ r_k = V\left[(I - CK)\tilde{y}_k - (I - CK)C\hat{x}_{k+1|k}\right], \end{cases} \quad (4)$$

Детектор отклонений синтезирован с применением подбора *K* и *V*:

1. В нормальном состоянии системы (т.е. $f_k = 0, \mathrm{u}_k = \tilde{u}_k, y_k = \tilde{y}_k$), ожидаемое значение сигнала последствия атаки r_k асимптотически сводится близко к нулю, т.е. $\lim_{k\to\infty} E\{\mathrm{r}_k\} \in \mathrm{B}_{\delta r}$, при $\delta_r \in R^+$ и $B_{\delta r} = \{r \in R^{n_r} : \|r\|_p \le \delta_r\}$;

2. Значение r_k чувствительно к возникновению аномальных отклонений $(f_k \neq 0)$.

Характеристика $B_{\delta r}$ зависит от шумов и может быть найдена в [3] для частных значений *p*.

Для заданного на временном интервале $[d_0, d_r]$ сигнала последствия атаки $\mathrm{r}_{[d_0, d_r]}$, генерируется сигнал тревоги если

$$\mathrm{r}_{[d_0, d_f]} \notin U_{[d_0, d_f]}, \quad (5)$$

где набор значений $U_{[d_0, d_f]}$ выбран так, чтобы уровень, соответствующий ложной тревоге, не достигал заданного порога $\alpha \in [0, 1]$. Последнее требует, чтобы тревоги не срабатывали в бесшумном, нормальном режиме функционирования системы (без атак), т.е. $\mathrm{r}_{[d_0, d_f]} \in U_{[d_0, d_f]}$, если для всех $k \in [d_0, d_f]$ выполняется условие $r_k \in B_{\delta r}$. Например, $U_{[d_0, d_f]}$ может быть введено как функция от энергии сигнала последствия атаки на интервале времени $[d_0, d_f]$, , что даст

$$U_{[d_0, d_f]} = \{r : \|r\|_{l2[d_0, d_f]} \le \delta\}.$$

Сетевая система автоматического управления под воздействием атаки

Пусть a_k – вектор сигнала атаки. Дополним состояния ОУ и АСУ $\eta_k = [x_k^T \; z_k^T]^T$, тогда динамика замкнутой системы, состоящей из *P* и *F*, под воздействием a_k может быть описана как

$$\eta_{k+1} = A\eta_k + Ba_k + G\begin{bmatrix} w_k \\ v_k \end{bmatrix},$$
$$\tilde{y}_k = C\eta_k + Da_k + H\begin{bmatrix} w_k \\ v_k \end{bmatrix}, \quad (4)$$

где матрицы системы заданы как

$$A = \begin{bmatrix} A + BD_cC_c & \\ B_cC & A_c \end{bmatrix},$$
$$G = \begin{bmatrix} G\; BD_c \\ 0 \quad B_c \end{bmatrix}, \quad C = [C\; 0], \quad H = [0\; I],$$

и *B*, и *D* отражает как вектор атаки a_k влияет на установку и контроллер.

Аналогично, используя *P* и *D*, как в (1) и (4), соответственно, динамика ошибок детектора отклонений при атаке описывается как

$$\xi_{k|k-1} = A_e\xi_{k|k-1} + B_e a_k + G_e\begin{bmatrix} w_k \\ v_k \end{bmatrix},$$
$$r_k = C_e\xi_{k|k-1} + D_e a_k + H_e\begin{bmatrix} w_k \\ v_k \end{bmatrix}, \quad (5)$$

где $\xi_{k|k-1} \in R^n$ предположительная ошибка и

$$A_e = A(I - KC), \quad G_e = [G - AK],$$
$$C_e = VC(I - KC), \quad H_e = [0 \;\; V(I - CK)].$$

Матрицы *Be* и *De* являются специфическими для доступных ресурсов атаки и описываются ниже.

Оценка целей и ограничений атак

Сценарии атак должны включать намерения противника, а именно цели атаки и ограничения, определяющие политику атаки. Цели атаки могут быть указаны с точки зрения воздействия атаки на работу системы, в то время как ограничения могут быть связаны с условиями обнаружения атак [14, 17].

Определение. Сигнал атаки $a_{[\mathrm{k}_o, k_f]}$ невидим на протяжении временного интервала $[k_0, d_f]$, при $d_f \ge k_f$, если $r_{[k_0, d_f]} \in u_{[k_0, \mathrm{d}_f]}$.

Отметим, что данная формулировка зависит от начального состояния системы в k_0, так же, как и от шумовых составляющих w_k и v_k. Более того, атака должна оставаться скрытой даже после окончания её воздействия, т.е. $d_f \ge k_f$.

Так как замкнутая система (6) и детектор отклонений (7) с учётом линейной стратегии атак являются линейными системами, каждая из этих систем может быть разделена на две составляющие: составляющую $a_k = 0 \forall k$ – соответствующую номинальному режиму работы системы, и следующие системы с нулевыми начальными состояниями $\eta_0^a = \xi_{0|0}^a = 0$

$$\eta_{k+1}^a = A\eta_k^a + Ba_k; \; \tilde{y}_k^a = C\eta_k^a + Da_k;$$
$$\xi_{k|k}^a = A_e\xi_{k-1|k-1}^a + B_e a_{k-1}; \; r_k^a = A_e\xi_{k-1|k-1}^a + D_e a_{k-1}.$$

Пусть система работала до атаки в номинальном режиме, и учитывая линейность (7), существует множество $u^a_{[k_0,\mathrm{d}_f]} \overset{\Delta}{=} \{r : \|r\|_{\ell_p[k_0,\mathrm{d}_f]} \le \delta_\alpha\}$ такое, что $r^a_{[k_0,\mathrm{d}_f]} \in U^a_{[k_0,\mathrm{d}_f]} \Rightarrow r_{[k_0,\mathrm{d}_f]} \in U_{[k_0,\mathrm{d}_f]}$, откуда может быть выведена следующая формулировка: сигнал атаки $a_{[\mathrm{k}_o, k_f]}$ не детектируем на интервале $[k_0, d_f]$, если $r^a_{[k_0,\mathrm{d}_f]} \in U^a_{[k_0,\mathrm{d}_f]}$.

Количественная оценка кибербезопасности: анализ установившегося состояния

Рассмотрим стационарность системы, находящийся под атакой.

Пусть $z \in \mathbb{C}$ и определяет

$$G_{xa}(z) = [I_n\, 0](zI - \mathbf{A})^{-1}\mathbf{B} + \mathbf{D},$$
$$G_{xa}(z) = C_e(zI - A)^{-1}B_e + D_e,$$

который соответствует переносу функций от a_k к x_k и r_k соответственно. Рассматривая сигналы атак $a_k = gz^k$ экспоненциальной формы для фиксированного z, обозначим $a(z) = g \in \mathbb{C}^{q_a}$, $x(z) = G_{xa}(z)a(z)$, и $r(z) = G_{ra}(z)a(z)$, как векторная запись a_k к x_k и r_k, соответственно.

Поскольку в данном разделе рассматривается только установившееся состояние системы, рассмотрим z как единичную окружность $z \in \mathbb{S}$, и таким образом $a(z)$ соответствует синусоидальному сигналу постоянной величины. Определяя в частотной области безопасное множество как $S^p_\infty = \{x \in \mathbb{C}^n : \|x\|_p \le 1\}$, система под воздействием атаки считается безопасной в установившемся состоянии если $x(z) = G_{xa}(z)a(z) \in S^p_\infty$.

Для данного $z \in S$, установившееся состояние влияния атаки описывается

$$g_p(x(z)) = \begin{cases} \|x(z)\|_p, \text{если } x(z) \in S^p_\infty, \\ +\infty, \text{в остальных случаях,} \end{cases} \quad (8)$$

Аналогично обратимся к множеству скрытых атак в установившемся состоянии $a(z)$ где $r(z) \in u^a \overset{\Delta}{=} \{r \in \mathbb{C}^{p_d} : \|r\|_p \le \delta_\alpha\}$, где $r(z) = G_{ra}(z)a(z)$.

Атаки, приводящие к максимальным воздействиям, могут быть вычислены решением

$\sup\limits_{z\in S} \max\limits_{a(z)} g_p(\mathrm{G}_{xa}(z)a(z))$, т.о. $\|G_{ra}(z)a(z)\|_p \le \delta_\alpha$.

Максимальное воздействие всех скрытых атак может быть подсчитано заменой целевой функции $g_p = G_{xa}(z)\,\mathrm{A}(z)$, при $\|G_{xa}(z)a(z)\|_p$, откуда

$$\sup_{z\in S} \max_{a(z)} \|\mathrm{G}_{xa}(z)a(z)\|_p, \text{т.о.} \quad (9)$$
$$\|G_{ra}(z)a(z)\|_q \le \delta_\alpha,$$

и таким образом, возможна оценка

$$g_p = (G_{xa}(z)a(z)).$$

Обеспечение кибербезопасности системы морского объекта на примере морского парома

Проиллюстрируем применение описанного метода для решения проблемы обеспечения безопасности АСУ балластной системы морского парома. На рисунке 2 приведено изображение интерфейса пользователя программы, разработанной авторами и функционирующей на указанном пароме, курсирующем по линии Крым – Кавказ [13, 14]. В результате модернизации, направленной на устранение проблем кренованием и дифферентованием судна, была разработана и введена информационная система автоматического управления балластом, интегрированная в общую сетевую систему контроля и мониторинга основных систем судна.

Балластная система парома была рассмотрена авторами в [1] и может быть описана системой уравнений

$$\begin{cases} \dot{h}_1 = -\dfrac{a_1}{A_1}\sqrt{2gh_1} + \dfrac{a_3}{A_1}\sqrt{2gh_3} + \dfrac{\gamma_1 k_1}{A_1}u_1, \\ \dot{h}_2 = -\dfrac{a_2}{A_2}\sqrt{2gh_2} + \dfrac{a_4}{A_2}\sqrt{2gh_4} + \dfrac{\gamma_2 k_2}{A_2}u_2, \\ \dot{h}_3 = -\dfrac{a_3}{A_3}\sqrt{2gh_3} + \dfrac{(1-\gamma_2)k_2}{A_3}u_2, \\ \dot{h}_3 = -\dfrac{a_4}{A_4}\sqrt{2gh_4} + \dfrac{(1-\gamma_1)k_1}{A_4}u_1, \end{cases}$$

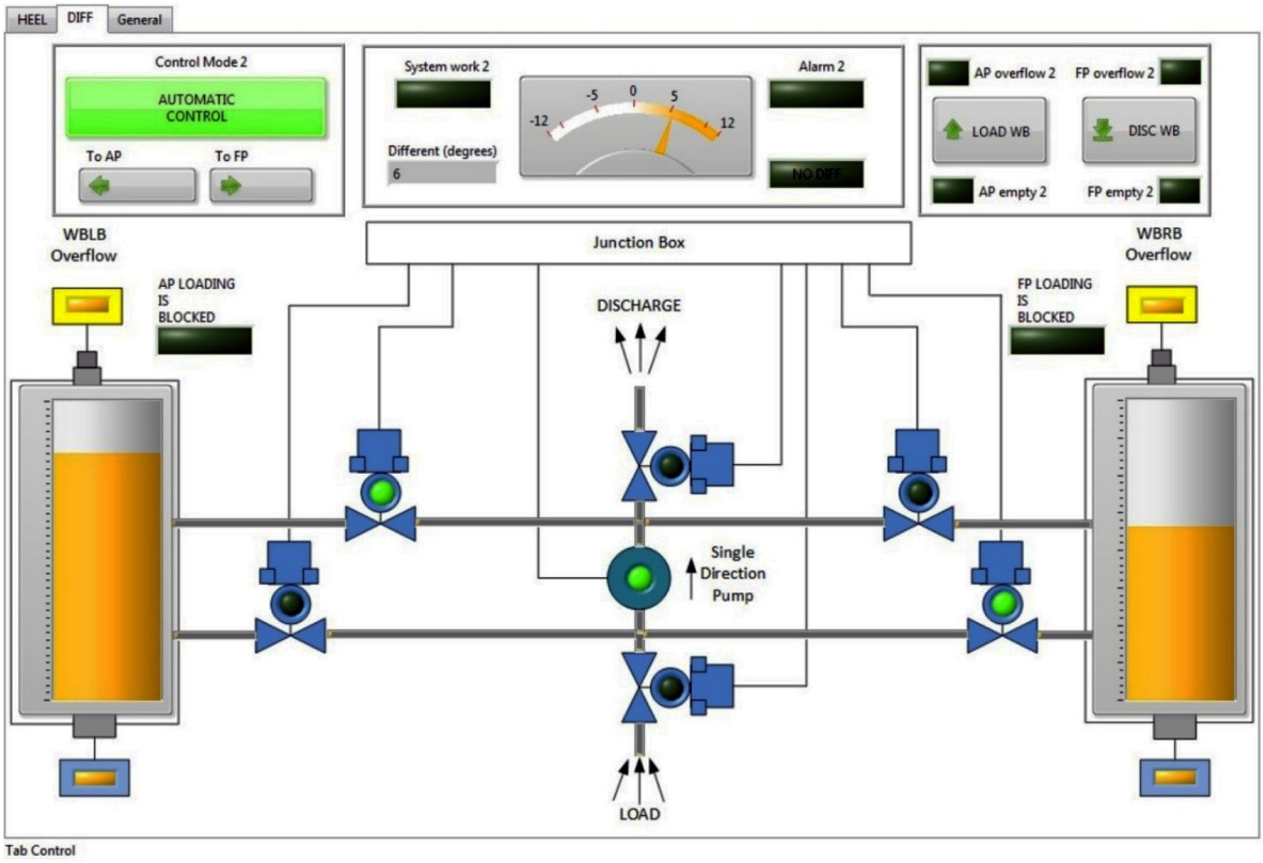

Рис.2. Интерфейс системы автоматического управления балластом критически важного морского объекта (панель управления кренованием)

где h_i – высоты воды в каждом резервуаре, A_i – площадь поперечного сечения резервуаров, a – площадь поперечного сечения выпускного отверстия, k_i – постоянные насоса, γ_i – коэффициенты расхода и g – ускорение силы тяжести.

Модель нелинейной установки линеаризуется для текущей рабочей точки. Состояния сигналов оцифровываются с периодом выборки Ts = 1 с. Для управления системой была разработана САУ с применением детектора аномалий на основе фильтра Калмана. Система настроена таким образом, чтобы сигнал тревоги вырабатывался согласно (5), при δα = 0,2.

В данной постановке в результате кибератаки могут быть искажены как данные о фактическом уровне воды в каждом из танков балластной системы, так и сигналы управления, регулирующие набор и сброс воды в каждом из танков. В результате намеренное искажение сигналов может привести к опрокидыванию судна или плавучей буровой платформы.

Для временного интервала [0, 30] атаки максимального воздействия с использованием минимального необходимого ресурса был рассчитан вариант протекания процесса при минимальной и неминимальной фазах путем итеративного решения (10) с $p = q = 2$. Было подтверждено, что неминимальное фазовое состояние системы менее устойчиво, чем минимальная фаза. В обоих случаях воздействие атаки может быть задано произвольно большим, с атакой по 3 и более каналам, и, таким образом, в исходной системе злоумышленник может вывести состояние из безаварийного, оставаясь скрытым.

Сигнал максимального воздействия для неминимальной фазовой системы с δα = 0,15 и p = q = 2 представлен на рисунке 3. Как видно, атака повреждает сигналы в двух каналах, и первая атака детектируется через секунду после её начала (на 17-й секунде), а вторая на 25 секунде.

Также видно, что детектор атак требует времени инициализации, на котором реакция на сигнал атаки должна быть отключена. Это время для расчётного случая составило 2-3 секунды. На время инициализации система не должна быть подвергнута атакам.

Дальнейшие исследования необходимым образом должны быть направлены на разработку методов изоляции и локализации атак для оперативного выявления источника и цели каждой конкретной атаки. Предложенные методы позволяют применить их в качестве базовых для решения подобных задач.

DOI:10.21681/2311-3456-2020-2-58-66

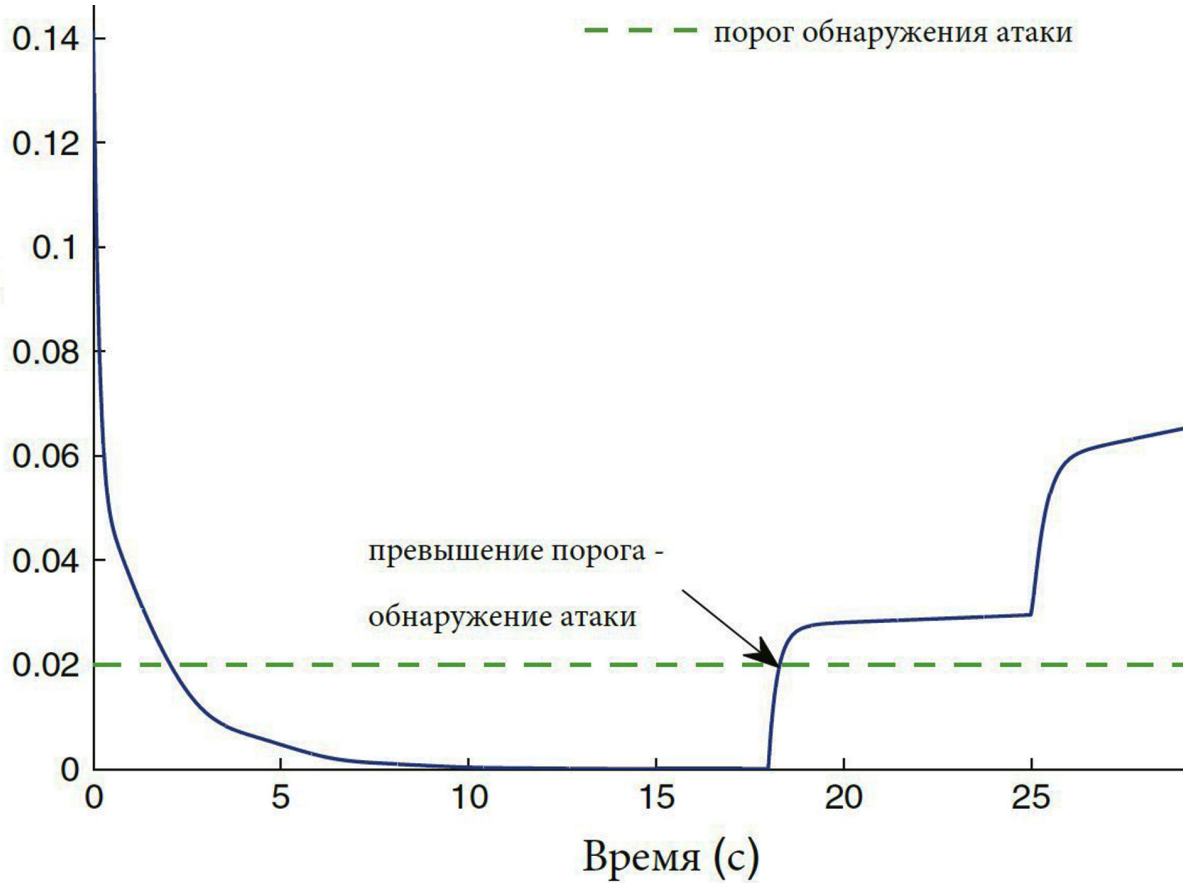

Рис. 3. Результат детектирования атаки максимального воздействия с ограниченными ресурсами, в неминимальном фазовом состоянии системы

Вывод

Предложены и сформулированы методики количественной оценки кибербезопасности сетевых систем управления. Рассмотрены проблемы с ограниченной оптимизацией, в которых учитываются условия между целями и ограничениями атакующего, такими как воздействие атаки на систему управления, обнаружение нападений и конкурирующие ресурсы. Показано, что предложенные оценки могут быть использованы для эффективного решения проблемы обеспечения кибербезопасности критического объекта.

Разработан алгоритм оценки атаки максимального уровня воздействия с ограничением ресурсов и сформулирована программа детектирования подобных атак. Результаты были проиллюстрированы на примере моделирования атаки на систему управления балластной системой морского объекта.

Рецензент: *Ловцов Дмитрий Анатольевич, Заслуженный деятель науки Российской Федерации, доктор технических наук, профессор, заведующий кафедрой информационного права, информатики и математики Российского государственного университета правосудия. Москва, Россия. E-mail: dal-1206@mail.ru*

Литература

1. Nyrkov A.P., Zhilenkov A.A., Sokolov S.S., Chernyi S.G. Hard- and software implementation of emergency prevention system for maritime transport // Automation and Remote Control. 2018. Т. 79. № 1. Pp. 195-202. DOI: 10.1134/S0005117918010174
2. Соколов С.С., Ныркov А.П., Чёрный С.Г., Жиленков А.А. Устройство контроля остойчивости судна. Патент на полезную модель RUS 169161 14.06.2016
3. Guo, B., Chen, Y. Adaptive fast sliding mode fault tolerant control integrated with disturbance observer for spacecraft attitude stabilization system // ISA Transactions. 2019. 94. Pp. 1-9. DOI: 10.1016/j.isatra.2019.04.014
4. Meng, Y., Jiang, B., & Qi, R. Adaptive fault-tolerant attitude tracking control of hypersonic vehicle subject to unexpected centroid-shift and state constraints // Aerospace Science And Technology. 2019. 95. Pp. 105515. DOI: 10.1016/j.ast.2019.1055155. Hu H., Liu L., Wang Y.,

Cheng Z., Luo, Q. Active fault-tolerant attitude tracking control with adaptive gain for spacecrafts // Aerospace Science and Technology. 2020. 98. Pp.105706. DOI: 10.1016/j.ast.2020.105706
5. Zhao Z., Jiang S., Ni, R., Fu S., Han Z., Yu Z. Fault-tolerant control of clutch actuator motor in the upshift of 6-speed dry dual clutch transmission // Control Engineering Practice. 2020. 95. Pp. 104268. DOI: 10.1016/j.conengprac.2019.104268
6. Liang, X., Wang, Q., Hu, C., Dong, C. Observer-based H∞ fault-tolerant attitude control for satellite with actuator and sensor faults // Aerospace Science and Technology. 2015. 95. Pp. 105424. DOI: 10.1016/j.ast.2019.105424
7. Ghanbarpour, K., Bayat, F., Jalilvand, A. Dependable power extraction in wind turbines using model predictive fault tolerant control // International Journal of Electrical Power & Energy Systems. 2020. 118. Pp.105802. DOI: 10.1016/j.ijepes.2019.105802
8. Li X., Wang, J. Fault-tolerant tracking control for a class of nonlinear multi-agent systems // Systems & Control Letters. 2019. 135. Pp. 104576. DOI: 10.1016/j.sysconle.2019.104576
9. Teixeira A., Shames I., Sandberg H., Johansson K. A secure control framework for resource-limited adversaries // Automatica. 2015. 51. Pp.135-148. DOI: 10.1016/j.automatica.2014.10.067
10. Van, M., & Do, X. Optimal adaptive neural PI full-order sliding mode control for robust fault tolerant control of uncertain nonlinear system // European Journal of Control. 2020. 21. DOI: 10.1016/j.ejcon.2019.12.005
11. Ding S.X. Model-based Fault Diagnosis Techniques: Design Schemes. Springer [Электронный ресурс]: 2015. URL: DOI: 10.1007/978-3-540-76304-8
12. Соколов С.С., Ныркov А.П., Чёрный С.Г., Жиленков А.А. Устройство контроля остойчивости судна. Патент на полезную модель RUS 165914 29.06.2016
13. Соколов С.С., Ныркov А.П., Чёрный С.Г., Жиленков А.А. Судовое балластное устройство. Патент на полезную модель RUS 160593 05.11.2015
14. Lei, R., & Chen, L. Adaptive fault-tolerant control based on boundary estimation for space robot under joint actuator faults and uncertain parameters // Defence Technology. 2019. 15(6). Pp. 964-971. DOI: 10.1016/j.dt.2019.07.010
15. Li, L., Luo, H., Ding, S., Yang, Y., Peng, K. Performance-based fault detection and fault-tolerant control for automatic control systems // Automatica. 2019. 99. Pp. 308-316. DOI: 10.1016/j.automatica.2018.10.047
16. Xiao, G., Liu, F. Distributed fault-tolerant model predictive control for intermittent fault: A cooperative way // ISA Transactions. 2019. 89. Pp. 113-121. DOI: 10.1016/j.isatra.2018.12.022

THE SYSTEM OF FAULT-TOLERANCE CONTROL OF CRITICAL OBJECTS OF MARITIME TRANSPORT IN THE CONTEXT OF CYBER ATTACKS

Zhilenkov A.A.[3], Chernyi S.G.[4]

The aim of the article is developing a number of approaches for quantifying cybersecurity of network control systems and detecting cyber-attacks on these one. Research method: the system under study is described by a model of discrete space-time with time-invariant feedback, the detection of attacks in which carried out using the proposed detection filter.

The possible goals and resource limitations of the attacker in the target control system, the effects of attacks are analyzed, and attack detection method is proposed. The analysis of component and cross-platform structures is carried out. Conclusions and structures of alignment and collision are made.

Research result: based on the proposed estimates of the maximum intensity of the possible impact, as well as sufficient and necessary resources for its implementation, an algorithm for detecting a cyber-attack on a network control system is proposed. The approach has several advantages of its implementation, one of which is the cost-effectiveness of implementation. The efficiency of the proposed approach is illustrated by the example of managing a critically important object of maritime transport. The developed practical examples are relevant and implemented in practice on ferries operating at the Kerch ferry. The implemented model allows to provide protection against cybernetic attacks on the ballast system of a critical marine transport facility.

Keywords: *maritime transport, cybersecurity, control system, ballast, restrictions, fault tolerance, discreteness.*

3 Anton A. Zhilenkov, Docent, Ph.D., Head of Department of Marine Electronics, St. Petersburg State Marine Technical University. IEEE member, DAAAM, St. Petersburg, Russia, E-mail: zhilenkovanton@gmail.com

4 Sergei Chernyi, Ph.D., Associate Professor, Department of Electrical Equipment for Ships and Automation Kerch State Maritime Technological University, Associate Professor Admiral Makarov State University of Maritime and Inland Shipping. Kerch, Russia. E-mail: sergiiblack@gmail.com

References

1. Nyrkov A.P., Zhilenkov A.A., Sokolov S.S., Chernyi S.G. Hard- and software implementation of emergency prevention system for maritime transport // Automation and Remote Control. 2018. Т. 79. № 1. Pp. 195-202. DOI: 10.1134/S0005117918010174
2. Соколов С.С., Ныркov А.П., Чёрный С.Г., Жиленков А.А. Устройство контроля остойчивости судна. Патент на полезную модель RUS 169161 14.06.2016
3. Guo, B., Chen, Y. Adaptive fast sliding mode fault tolerant control integrated with disturbance observer for spacecraft attitude stabilization system // ISA Transactions. 2019. 94. Pp. 1-9. DOI: 10.1016/j.isatra.2019.04.014
4. Meng, Y., Jiang, B., & Qi, R. Adaptive fault-tolerant attitude tracking control of hypersonic vehicle subject to unexpected centroid-shift and state constraints // Aerospace Science And Technology. 2019. 95. Pp. 105515. DOI: 10.1016/j.ast.2019.1055155. Hu H., Liu L., Wang Y., Cheng Z., Luo, Q. Active fault-tolerant attitude tracking control with adaptive gain for spacecrafts // Aerospace Science and Technology. 2020. 98. Pp.105706. DOI: 10.1016/j.ast.2020.105706
5. Zhao Z., Jiang S., Ni, R., Fu S., Han Z., Yu Z. Fault-tolerant control of clutch actuator motor in the upshift of 6-speed dry dual clutch transmission // Control Engineering Practice. 2020. 95. Pp. 104268. DOI: 10.1016/j.conengprac.2019.104268
6. Liang, X., Wang, Q., Hu, C., Dong, C. Observer-based H∞ fault-tolerant attitude control for satellite with actuator and sensor faults // Aerospace Science and Technology. 2015. 95. Pp. 105424. DOI: 10.1016/j.ast.2019.105424
7. Ghanbarpour, K., Bayat, F., Jalilvand, A. Dependable power extraction in wind turbines using model predictive fault tolerant control // International Journal of Electrical Power & Energy Systems. 2020. 118. Pp.105802. DOI: 10.1016/j.ijepes.2019.105802
8. Li X., Wang, J. Fault-tolerant tracking control for a class of nonlinear multi-agent systems // Systems & Control Letters. 2019. 135. Pp. 104576. DOI: 10.1016/j.sysconle.2019.104576
9. Teixeira A., Shames I., Sandberg H., Johansson K. A secure control framework for resource-limited adversaries // Automatica. 2015. 51. Pp.135-148. DOI: 10.1016/j.automatica.2014.10.067
10. Van, M., & Do, X. Optimal adaptive neural PI full-order sliding mode control for robust fault tolerant control of uncertain nonlinear system // European Journal Of Control. 2020. 21. DOI: 10.1016/j.ejcon.2019.12.005
11. Ding S.X. Model-based Fault Diagnosis Techniques: Design Schemes. Springer [Электронный ресурс]: 2015. URL: DOI: 10.1007/978-3-540-76304-8
12. Соколов С.С., Ныркov А.П., Чёрный С.Г., Жиленков А.А. Устройство контроля остойчивости судна. Патент на полезную модель RUS 165914 29.06.2016
13. Соколов С.С., Ныркov А.П., Чёрный С.Г., Жиленков А.А. Судовое балластное устройство. Патент на полезную модель RUS 160593 05.11.2015
14. Lei, R., & Chen, L. Adaptive fault-tolerant control based on boundary estimation for space robot under joint actuator faults and uncertain parameters // Defence Technology. 2019. 15(6). Pp. 964-971. DOI: 10.1016/j.dt.2019.07.010
15. Li, L., Luo, H., Ding, S., Yang, Y., Peng, K. Performance-based fault detection and fault-tolerant control for automatic control systems // Automatica. 2019. 99. Pp. 308-316. DOI: 10.1016/j.automatica.2018.10.047
16. Xiao, G., Liu, F. Distributed fault-tolerant model predictive control for intermittent fault: A cooperative way // ISA Transactions. 2019. 89. Pp. 113-121. DOI: 10.1016/j.isatra.2018.12.022