УДК: 004.056.53
Оригинальная статья
Надежность, том 18, №4, 2018 DOI: 10.21683/1729-2646-2018-18-4-36-44

Методика оценки защищенности микропроцессорных систем управления в условиях информационно-технических воздействий

Сергей М. Климов, *4 ЦНИИ Минобороны России, Королёв, Россия*
Юрий В. Сосновский, *Физико-технический институт Крымского федерального университета им. В.И. Вернадского, Симферополь, Россия*

Сергей М. Климов

Юрий В. Сосновский

Резюме. *Целью статьи является разработка моделей, позволяющих дать типовое представление структуры, функций микропроцессорных систем управления (МСУ) и получить количественную оценку рисков (отказоустойчивости) автоматизированных систем управления и их основных компонент – МСУ в условиях информационно-технических воздействий (ИТВ). В статье показана актуальность и важность моделей МСУ и оценки рисков функционирования автоматизированных систем управления технологическими процессами (АСУ ТП) при осуществлении на них различных ИТВ (компьютерных атак). В качестве ИТВ нарушителя рассматриваются аппаратные, аппаратно-программные и программные воздействия, обладающие свойствами блокирования коммуникационных каналов, нарушения доступности и целостности информации, а также целенаправленного и продолжительного информационно-технического воздействия на автоматизированную систему, в том числе, вредоносными программами. Разработанная в статье структурно-функциональная модель микропроцессорной системы управления как основной компоненты системы более высокого уровня – АСУ ТП, образована совокупностью схем и описаний функций. Структурно-функциональная модель включает в свой состав: структуры каналов основного цикла системы управления (считывание данных, обработка, запись выходных значений, а также работа с коммуникационной подсистемой), структурно-функциональную схему МСУ различного типа в зависимости от наличия и уровня использования телекоммуникационного канала в структуре цикла управления, типового паспорта уязвимости МСУ. В схемах подробно описаны типовые функции, порядок работы и информационного взаимодействия модулей МСУ с внешней средой через каналы передачи данных. Модель рисков АСУ ТП и МСУ, как ее части, в условиях воздействий ИТВ описывается показателями, характеризующими условный ущерб и состояние системы управления, при котором она может восстановить свою работоспособность или потребуется внешнее вмешательство, затрагивающее не только саму систему управления, но контролируемый технологический процесс. В качестве показателей, рассмотрены следующие: характеристические точки и параметры функции риска, основанной на распределении Вейбулла-Гнеденко, статистическая оценка защищенности МСУ, функция риска, динамическая оценка риска успешной реализации ИТВ на МСУ. Предполагается, что значения параметров, необходимых для расчета показателей риска и защищенности МСУ получены:*
- эмпирически, на основе структурно-параметрического анализа особенностей построения, динамики функционирования и уязвимостей МСУ;
- в рамках имитационного моделирования МСУ как абонентов вычислительных сетей в условиях ИТВ на стендовом полигоне;
- экспериментально на основании частоты успешно реализованных угроз ИТВ,
а также показатели защищенности экстраполируются на весь жизненный цикл МСУ посредством введения динамической поправки, основанной на функции риска с использованием распределения Вейбулла-Гнеденко.
В выводе отмечается, что разработанная методика оценки защищенности МСУ в условиях ИТВ позволяет оценить риски успешной реализации нарушителем вредоносного воздействия на МСУ и АСУ ТП в целом, что создает предпосылки для своевременного устранения уязвимостей в МСУ и принятия дополнительных организационно-технических мер по повышению уровня информационной безопасности автоматизированных систем управления.

Ключевые слова: *информационно-технические воздействия, микропроцессорные системы управления, средства защиты информации, отказоустойчивость.*

Формат цитирования: Климов С.М., Сосновский Ю.В. Методика оценки защищенности микропроцессорных систем управления в условиях информационно-технических воздействий // Надежность. 2018. № 4. С. 36-44. DOI: 10.21683/1729-2646-2018-18-4-36-44

Введение

Доктриной информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации 2016 года, определены современные угрозы информационно-технических воздействий на критическую информационную инфраструктуру страны.

В настоящее время необходимость развития цифровой экономики страны обусловливает активное внедрение информационных и коммуникационных технологий в автоматизированных системах управления технологическими процессами (АСУ ТП). За рубежом АСУ ТП классифицируются как SCADA-системы для управления энергетикой, транспортом и промышленными системами. На практике внедрение информационных и коммуникационных технологий приводит к появлению дополнительных уязвимостей в программном обеспечении, что повышает вероятность реализации на них нарушителем угроз информационно-технических воздействий (ИТВ).

Современные средства реализации ИТВ вредоносными программами [1], например, Stuxnet, Flame, miniFlame, Duqu, Gauss, Reign, Wiper, Shamoon, Careto используют уязвимости программного кода АСУ ТП для скрытного внедрения, самораспространения и целенаправленного нарушения функционирования системы. Развитие средств ИТВ и их функциональных возможностей значительно опережает разработку соответствующих средств обнаружения предупреждения компьютерных атак (СОПКА), особенно в форме вредоносных программ.

Ключевым элементом СОПКА для АСУ ТП является сенсор (индикаторный программно-аппаратный или программный модуль) регистрирующий факт компьютерного инцидента – успешной реализации ИТВ нарушителем.

Базовым элементом АСУ ТП являются микропроцессорные системы управления (МСУ) [2], программное обеспечение которых выполняет функции сбора, обработки и передачи информации для управления в реальном масштабе времени критически важными объектами. Если ранее программируемые производственные микропроцессоры управлялись набором специальных команд, то на современном уровне они функционируют под управлением операционных систем (ОС) общего применения (например, ОС Windows или Linux) и доступны как абоненты вычислительной сети с протоколами передачи данных типа TCP/IP или с характерным для SCADA-систем протоколом Modbus.

Для оценки и обеспечения защиты информации в МСУ в условиях реализации угроз ИТВ нарушителем необходим комплекс методик и средств для обнаружения, идентификации вредоносных воздействий и ликвидации их последствий [9-14].

Таким образом, задача разработки методики оценки защищенности МСУ в условиях ИТВ с целью априорной количественной оценки рисков нарушения функционирования МСУ критически важных объектов является актуальной и представляет практический интерес.

Постановка задачи

При проведении исследований были приняты следующие допущения:

- оценка рисков успешных ИТВ нарушителя должна выполняться на стендовом полигоне, позволяющем создать требуемые тестовые условия для работы функциональных аналогов МСУ, элементов СОПКА и имитации ИТВ;

- выделенные группы рисков нарушения функционирования МСУ возможно оценивать непосредственно на объекте с помощью мобильного тестового комплекса;

- предварительная оценка уязвимостей МСУ и угроз ИТВ нарушителя позволяет сформировать возможные варианты средств защиты информации (СЗИ) и выбрать наиболее эффективный из них.

Параметры защищенности МСУ определяются:

- эмпирически, на основе структурно-параметрического анализа особенностей построения, динамики функционирования и уязвимостей МСУ;

- экспериментально на основании частоты успешно реализованных угроз ИТВ нарушителя,

при этом установленные показатели защищенности экстраполируются на весь жизненный цикл МСУ посредством введения динамической поправки, основанной на функции риска с использованием распределения Вейбулла-Гнеденко [3-4].

Основой для разработки методики оценки защищенности МСУ в условиях ИТВ является модель функционирования МСУ в условиях ИТВ, которая позволяет проводить комплексный анализ взаимосвязанных процессов функционирования МСУ, реализации ИТВ и ликвидации их последствий.

В разработанной модели предполагается, что МСУ оснащена коммуникационной подсистемой. Коммуникационная подсистема выполняет такие функции, как взаимодействие с промышленными системами более высокого уровня, удаленное считывание данных с датчиков и запись их значений в исполнительные устройства посредством сетевых интерфейсов.

Коммуникационная подсистема МСУ, которая напрямую включена в контур управления технологическим процессом, и является основной уязвимостью для реализации нарушителем угроз ИТВ на ее протоколы передачи данных. Предполагается, что при реализации ИТВ нарушителем могут быть использованы недекларированные возможности как в аппаратно-программных средствах МСУ, так и в программируемых маршрутизаторах сети передачи данных на различных уровнях АСУ ТП. Кроме того, нарушитель может быть не только внешний, но и внутренний, который знаком со спецификой и временными ограничениями технологического процесса (условиями срабатывания автоматических и автоматизированных

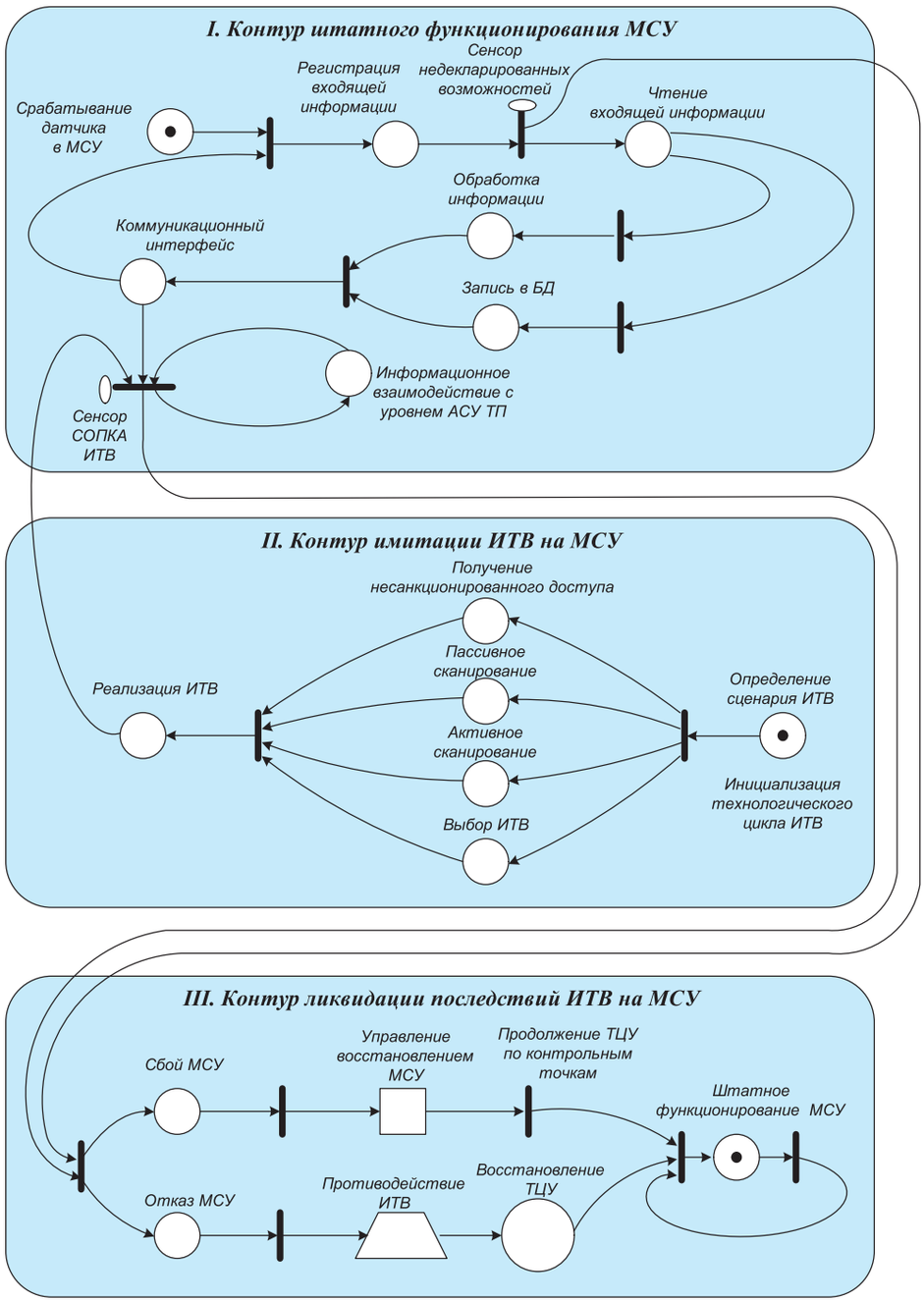

Рисунок 1 – Схема модели функционирования МСУ в условиях ИТВ и терминах РСП

исполнительных устройств), и способен реализовать неизвестное воздействие «нулевого» дня.

Схема модели функционирования МСУ в условиях ИТВ и терминах расширенной сети Петри (РСП) [5] представлена на рисунке 1.

Модель функционирования МСУ в условиях ИТВ включает в свой состав три контура:

1. Контур штатного функционирования МСУ, позволяющий осуществить имитационное моделирование и структурно-параметрический анализ технологического цикла управления (ТЦУ) МСУ.

2. Контур имитации ИТВ, предназначенный для моделирования действий нарушителя по получению несанкционированного доступа к МСУ, пассивного и активного сканирования уязвимостей, выбора и запуска ИТВ. В качестве исходных данных о современных угрозах ИТВ нарушителя вредоносными программами в статье использованы материалы статьи [1].

3. Контур ликвидации последствий ИТВ, обеспечивающий моделирование процессов предупреждения, обнаружения и ликвидации последствий ИТВ на основе использования сенсоров (индикаторных модулей) обна-

ружения и идентификации воздействий.

На рисунке 1 в блоке III показаны две альтернативы ликвидации последствий ИТВ на МСУ в случае их успешной реализации нарушителем.

Ветвь I (верхняя) отражает ситуацию, при которой МСУ обладает свойством восстановления в случае сбоя (относительно кратковременной ТЦУ – от нескольких секунд до нескольких минут). Под сбоем понимается кратковременное нарушение ТЦУ, вызванное ИТВ, но не приводящее к срыву работы МСУ. В этом случае при идентификации сбоя в системе запускается алгоритм восстановления ТЦУ, после выполнения которого МСУ переходит в состояние нормального функционирования.

Ветвь II (нижняя) иллюстрирует такой исход реализации ИТВ нарушителем, при котором МСУ переходит в состояние отказа, характеризующегося длительным нарушением процессов управления в МСУ (от 30 минут до нескольких часов).

Специфика МСУ такова, что восстановление ТЦУ после длительного отказа зачастую требует вмешательства оператора и (или) технического персонала и не может быть выполнено перезапуском или внедрением заведомо работоспособной МСУ.

Для предотвращения сбоев и отказов в МСУ в условиях ИТВ необходимо оперативное обнаружение, локализация воздействия и восстановление ТЦУ на основе внедренных избыточных сенсоров (индикаторных программно-аппаратных средств) СОПКА [5-6].

Формализация модели функционирования МСУ в условиях ИТВ и терминах РСП [5]:

$$S_{МСУ} = \{(P,V),T,D,M,Q,I_p,Y\}, \quad (1)$$

где $P = p_1, p_2, ..., p_i$ – непустое конечное множество позиций, характеризующих штатный режим функционирования МСУ;

$V = v_1, v_2, ..., v_i$ – множество позиций восстановления, отражающие процедуры восстановления после успешных ИТВ нарушителя (графически представляется □);

$T = t_1, t_2, ..., t_i$ – непустое множество переходов, при этом в соответствии с РСП каждому переходу t_i может быть поставлен в соответствии алгоритм его срабатывания $a \vee g_i$ (при наличии алгоритма над переходом делается пометка $a \vee g_i$);

D – непустое конечное множество дуг сети, причем $D = (D_1 \cup D)$, $D_1 = (P \times T) \cup (V \times T)$ – непустое множество входных дуг, соединяющих позиции и переходы, $D_2 = (T \times P) \cup (T \times V)$ – непустое множество выходных дуг, ориентированных от переходам к позициям;

M – множество маркировок сети Петри;

$F_p : (M_p : P \to N), F_v : (M_v : V \to N)$ – функции начальной маркировки позиций штатного функционирования и восстановления, соответственно, N={0,1,2,…} – множество натуральных чисел (помечается точкой внутри позиции ⊙);

Q – множество вероятностей запусков переходов, отражающее вероятности нахождения МСУ в режиме штатного функционирования, моменты реализации ИТВ и срабатывания датчиков СОПКА, процессы восстановления;

$Z_{АПДi}$ – множество позиций противодействия ИТВ ( );

$I_p = i_{p1}, i_{p2}, ..., i_{pm}$ – множество приоритетов для дуг;

$Y = y_1, y_2, ..., y_k$ – множество временных параметров ИТВ.

Функции описания структуры РСП в виде отображения множеств выглядят как

$$F_{d1} : P \times T \bigcup V \times T \to N, \text{ или } F(p_i, v_j, t_n), \quad (2)$$

$$F_{d2} : T \times P \bigcup T \times V \to N, \text{ или } F(t_n, p_i, v_j),$$

где F_{d1} – функция входных позиций, ставящая в соответствие позициям и переходам количество маркеров, необходимых для запуска перехода («входа»);

F_{d2} – функция выходных позиций, ставящая в соответствие позициям и переходам количество маркеров, необходимых для изменения маркировки (корректировки «выхода»);

N={0,1,2,…} – множество натуральных чисел.

С учетом вышесказанного, правило запуска переходов имеет общий вид:

$$\forall (p_i \in P \wedge v_j \in V) \to \exists (M(p_i) \geq F_{d1}(p_i, v_j, t_n)). \quad (3)$$

Если сработал переход t_n, то из каждой его входной позиции p_i и v_j удаляется количество маркеров $m(p_i)$ и $m(v_j)$, равное числу входных дуг, а в выходные позиции p_{i+1} и v_{j+1} добавляется число маркеров, равное числу выходных дуг. При этом происходит срабатывание перехода, которому соответствует наибольшее значение вероятности его запуска (q_w) и предшествует дуга с более высоким приоритетом (i_{pm}). Задержка на время срабатывания перехода определяется параметрами ИТВ (y_k) в позициях сети, из которых выходят дуги к этому переходу. С учетом этого, правило изменения маркировки РСП имеет вид:

$$\forall (M_p \wedge M_v) : (p_i \in P \wedge v_j \in V) \to \exists (M'_p \wedge M'_v) =$$
$$= F_p(Mp) + F_v(Mv) - F_{d1}(p_i, v_j, t_n) + F_{d2}(t_n, p_i, v_j). \quad (4)$$

Описание начальной маркировки (M_i) в РСП для отображения и анализа причинно-следственных связей между процессами в МСУ и системы СОПКА при воздействии ИТВ. Условие достижимости РСП:

$$\forall (p_i \in P \wedge V_r \in V \wedge Z_j \in Z_{АПД}) \to \exists M'(p_i, v_r, z_j) =$$
$$= M(p_i, v_r, z_j) - [F_p(M_p) + F_v(M_v) + F_z(M_z)] -$$
$$- [F_{ud1}(p_i, v_r, z_j, t_n) + F_{ud2}(t_n, p_i, v_r, z_j)]. \quad (5)$$

Определение логических условий для срабатывания переходов РСП (T_i) при маркировке $M(p_i, v_r, z_j)$:

$$\forall\left(p_i \in P \wedge V_r \in V \wedge Z_j \in Z_{АПД}\right) \rightarrow$$
$$\rightarrow \exists\left[M\left(p_{i1}, v_{r1}, z_{j1}\right) \geq F_{ud1}\left(p_i, v_r, z_j, t_n\right)\right],$$
$$\Psi_t\left[\left(p_{i1}, v_{r1}, z_{j1}\right),...,\left(p_{in}, v_{rn}, z_{jn}\right)\right] = 1, \quad (6)$$

где Ψ_t – функция распределения маркировки по входным позициям РСП.

Определение соотношения для позиции РСП – «подсобытий» $P_i, V_r, Z_{АПДi}$ предупреждения, обнаружения, анализа ИТВ, активного противодействия им, а также восстановления МСУ:

$$\forall\left(p_i \in P, e_i \in E_{ki}, n_i \in N_{ki}, b_i \in B_{ki}\right) \rightarrow$$
$$\rightarrow \exists \min\left(p_i, V_r, Z_j, E_{ki+1}, N_{ki+1}, B_{ki+1},\right) \rightarrow$$
$$\rightarrow Z^*_{\text{ПД}} \rightarrow, \Psi_{tn} = \left\{\left(p_{i1}, V_{r1}, Z_{j1}\right),...,\left(p_{in}, V_{rn}, Z_{jn}\right)\right\}. \quad (7)$$

Функция начального входного распределения маркировки Ψ_t по позициям РПС принимает значения (8), которое определяет порядок начального размещения маркеров по позициям РСП

$$\Psi_{tn}\left(p_i, V_r, Z_j\right) = \left\{1, \textit{если } m_{pi} \in M_p, m_{vr} \in M_v, m_{zj} \in M_z. \right. \quad (8)$$

Задание условия срабатывания сенсоров СОПКА (Q_i):

$$\forall t_i \in T, Q_{ki} \in Q, \exists Q_{i+1} \neq 0,$$
$$\phi_q\left(t_i, Q_{ki}\right) = \left\{1, \textit{если } mp_i \in M_p, y_i \in Y, a \vee g_i = \right.$$
$$= 1, \left\{\frac{1}{R}, \textit{если } mp_i \in M_p, y_i \notin Y, a \vee g_i = 1, \right. \quad (9)$$

где $a \vee g_i$ – алгоритм срабатывания сенсора. Условия срабатывания сенсора выглядят следующим образом:

$\phi_q\left(t_i, Q_{ki}\right) = 1$ – сенсор сработал, атака обнаружена;

$\phi_q\left(t_i, Q_{ki}\right) = \frac{1}{R}$ – ложное срабатывание сенсора при R-ном срабатывании перехода;

$\phi_q\left(t_i, Q_{ki}\right) = 0$ – сенсор не сработал, неизвестная атака не обнаружена.

С учетом современных методов защиты информационных систем и управления рисками [1, 5, 7, 9, 13, 14] методика оценки защищенности МСУ в условиях ИТВ представлена в виде последовательности шагов:

1. Определение способа мониторинга МСУ с учетом особенностей функционирования (контролируемых процессов и типов протоколов передачи данных).

2. Анализ уязвимостей и формирование паспорта уязвимостей МСУ.

3. Разработка модели угроз ИТВ.

4. Разработка имитационной модели контролируемого ТЦУ в МСУ с учетом коммуникационных интерфейсов АСУ ТП.

5. Проведение экспериментальных исследований МСУ в условиях ИТВ на основе имитационного моделирования на стендовом полигоне.

6. Оценка показателей защищенности МСУ по результатам моделирования.

7. Оценка рисков нарушения защищенности МСУ в условиях ИТВ.

Шаг 1. Способ мониторинга МСУ основывается на классификации МСУ. Классификация МСУ выполняется по признакам, включающим в себя определение наличия проводных и беспроводных коммуникационных каналов, интерфейсов (однонаправленность, двунаправленность, «многоточка»), возможности удаленной «перепрошивки» программного обеспечения и удаленного администрирования МСУ. По указанным признакам, выделим базовые типы МСУ:

МСУ 1-го типа – система с локальным контроллером, осуществляющая локальное чтение входных сигналов, обработку данных и выработку выходных управляющих сигналов с помощью локальных модулей вывода;

МСУ 2-го типа – система, использующая интерфейсы передачи данных в качестве информационной среды между удаленными модулями ввода-вывода и процессорными блоками;

МСУ 3-го типа – системы, использующие протоколы передачи данных, функционирующие в двунаправленном варианте для передачи данных на системы более высокого уровня и прием данных от них;

МСУ 4-го типа – системы, обладающие перечисленными особенностями 3-го типа но, кроме этого, допускающие возможность удаленного (с использованием общей среды передачи данных) администрирования, в том числе – корректировки и смены управляющей программы («перепрошивки»).

К контролируемым процессам относится внутренний и внешний обмен данными через интерфейсы МСУ, параметры сетевого трафика с элементами АСУ ТП. Мониторинг обмена в МСУ разделен по типам протоколов передачи данных и осуществляется сенсорами СОПКА сигнатурным анализом и функциональным анализом аномального поведения МСУ, выявлением искажений структуры протоколов, параметров сигнализации и синхронизации, преамбулы пакетов данных и различных служебных параметров оборудования МСУ.

Шаг 2. Уязвимости программного обеспечения МСУ определим с использованием ГОСТ Р 56546-2015 [8] и формализуем в виде типового паспорта уязвимостей программного обеспечения МСУ в условиях ИТВ (таблица 1). За основу взят паспорт уязвимостей базы данных ФАУ «ГНИИИ ПТЗИ ФСТЭК России» BDU:2018-00543. В качестве дополнения к типовому паспорту уязвимостей требуется введение следующих характеристик:

1. Тип промышленного протокола передачи данных (ввиду потенциально возможных уникальных атак на промышленные протоколы с учетом их аппаратной и программной специфики).

2. В вектор уязвимости ввести данные, касающиеся контролируемого технологического процесса (обычный, важный, критически важный), так как информационно-

Таблица 1 – Типовой паспорт уязвимости (на примере BDU:2018-00543)

Описание уязвимости	Уязвимость сценария track_import_export.php системы управления производственными и жилыми объектами U.motion builder связана с непринятием мер по защите структуры SQL-запроса
Вендор	Schneider Electric
Наименование ПО	U.motion Builder
Версия ПО	до 1.3.4
Тип ПО	Программное средство АСУ ТП
ОС и аппаратные платформы	Данные уточняются
Тип ошибки	Непринятие мер по защите структуры запроса SQL (атаки типа \»внедрение SQL\»)
Идентификатор типа ошибки	CWE-89
Класс уязвимости	Уязвимость кода
Дата выявления	02.03.2018
Базовый вектор уязвимости	AV:N/AC:L/Au:N/C:C/I:C/A:C
Уровень опасности уязвимости	Критический уровень (базовая оценка CVSS 2.0 составляет 10) Высокий уровень (базовая оценка CVSS 3.0 составляет 8,8)
Возможные меры по устранению уязвимости	Использование рекомендаций: https://www.schneider- electric.com/en/download/document/SE_UMOTION_BUILDER/
Статус уязвимости	Подтверждена производителем
Наличие эксплойта	Данные уточняются
Способ эксплуатации	Инъекция
Способ устранения	Обновление программного обеспечения
Информация об устранении	Уязвимость устранена
Ссылка на источники	https://www.schneider-electric.com/en/download/document/SE_UMOTION_BUILDER/
Идентификаторы других систем описания уязвимостей	CVE: CVE-2018-7765
Прочая информация	

техническое воздействие на МСУ, АСУ ТП приводит не только к сбою или отказу данной системы, а влечет за собой сбой или отказ контролируемого технологического процесса.

3. Показатель «Уровень опасности уязвимости» зависит как от уровня угрозы уязвимости, так и от типа контролируемого технологического процесса (обычный, критически важный).

Шаг 3. Разработка модели угроз ИТВ основана на анализе потенциальных угроз, зависящих от типа МСУ (по классификации), а также используемых протоколов и контролируемых технологических циклов управления (ТЦУ).

Ввиду того, что рассматривается безопасность информации уровня МСУ, можно выделить следующие основные пути реализации угроз ИТВ нарушителя:

- угрозы информационного воздействия, приходящие с более высокого уровня АСУ ТП (такими угрозами могут быть некорректные значения уставок для данного технологического процесса, принудительная их фиксация, иные попытки нарушить работу МСУ посредством искажения информации и управляющих параметров);

- угрозы воздействия на протоколы ввода и вывода информации в МСУ (в случае отнесения последней к МСУ 2-4 типов), приводящие к блокировке протоколов или нарушения целостности передаваемых данных;

- угрозы воздействия на программную составляющую МСУ (при наличии возможности удаленной «перепрошивки» контроллеров).

Возможности реализации угроз ИТВ нарушителя непосредственно связаны с характеристиками используемого оборудования, протоколов, контролируемых технологических процессов в МСУ и не могут рассматриваться вне данного контекста.

Шаг 4. Разработка имитационной модели контролируемого ТЦУ в МСУ (объекта исследований) с учетом коммуникационных интерфейсов АСУ ТП заключается в разработке так называемого «информационного окружения» и базовых функций для МСУ. В ходе экспериментальных исследований на стенде модель ТЦУ может быть представлена отдельной группой программируемых устройств, например программируемыми логическими коммутаторами, программы которых позволяют моделировать ТЦУ в МСУ при изменении преднамеренных и непреднамеренных управляющих и информационных воздействий. При имитационном моделировании роль «информационного окружения» играют независимые программные блоки модели, а при натурном моделировании – реальное оборудование, за-

Таблица 2 – Дополненные показатели, характеризующие проектную защищенность МСУ

Структурно-функциональные характеристики МСУ	Уровень проектной защищенности МСУ		
	Высокий	Средний	Низкий
По типу взаимодействия между уровнями МСУ: - автономная, нет межуровневого взаимодействия, есть однонаправленное (на верхний уровень); - есть двунаправленное взаимодействие.	3	2	-
По организации интерфейсов ввода-вывода: - локальные физические (электрические) подключения; - используются коммуникационные интерфейсы, они физически отделены от иных сегментов сети; - общая коммуникационная среда.	3	2	1
Наличие средств «перепрошивки» программного обеспечения МСУ: - отсутствует; - имеется, требует локального подключения; - возможность удаленного управления.	3	2	1
По встроенным средствам контроля МСУ и самодиагностики: - отсутствуют; - имеется идентификация сбоя (отказа); - имеется идентификация сбоя (отказа), средства восстановления работоспособности и резервирования функций.	3	2	1

действованное в контроле ТЦУ. В рамках моделирования сам реальный ТЦУ в МСУ может быть не запущен (ввиду сложности полного воспроизведения функций АСУ ТП), а моделирование его реакции на те или иные воздействия может осуществляться добавлением независимых программных модулей в специальное программное обеспечение коммуникационного оборудования.

Шаг 5. Проведение экспериментальных исследований МСУ в условиях ИТВ на основе имитационного моделирования на стендовом полигоне основано на выполнении трех основных процессов:

- моделирование штатного функционирования МСУ;

- имитация ИТВ на МСУ из базы данных моделей воздействий;

- моделирование СЗИ, в качестве которых в статье рассматриваются сенсоры СОПКА, настроенные на мониторинг ТЦУ с учетом предложенной классификации МСУ.

Программный код и сценарий для имитации ИТВ хранится в базе данных и разрабатывается с учетом используемых протоколов, типов и потенциальных уязвимостей МСУ (согласно классификации). Ряд ИТВ может быть представлен стандартными компьютерными атаками, например ARP-спуфинг, DDoS-атаки, другие же являются специфическими для применяемых в АСУ ТП протоколов. Примерами специальных ИТВ могут являться компьютерные атаки на протокол синхронизации времени PTP (IEEE 1588), протокол Modbus, встроенное программное обеспечение контроллера МСУ.

Шаг 6. Статистическая оценка защищенности МСУ состоит в проведении оценки защищенности МСУ по результатам имитационного и натурного моделирования. Оценка защищенности МСУ строится на контроле корректности функционирования системы управления по уровням эталонной модели взаимодействия открытых систем.

Для расчета показателей статистической оценки защищенности МСУ используется принцип ALARP и четыре установленные категории риска: от недопустимого до не принимаемого в расчет [13, 14]. Соответственно, для каждого типа ИТВ и заданного (эмпирически или полученного путем моделирования) выбирается уровень допустимого риска и коэффициент относительного шага шкалы риска, позволяющий формализовать отнесения последствий реализации ИТВ к одной из четырех категорий риска, принятых согласно принципу ALARP, также индивидуально для каждого типа ИТВ выбираются значения функции значимости.

С учетом изложенного, итоговая интегральная оценка риска системы может рассчитываться по формуле

$$R_{МСУ} = \frac{\sum_{j=0}^{3} k_j z_j w_j}{RS}, \qquad (10)$$

где k_j – количество ИТВ с уровнем риска j;

z_j – значение функции значимости соответствующего риска;

w_j – условный вес соответствующего уровня риска;

$RS = N \cdot k_3 \cdot w_3$, N – число типов реализуемых ИТВ согласно модели угроз.

Кроме того, в методике предлагается учитывать уровень проектной защищенности МСУ, соответствующий ее структурным построением и функциональным возможностям, определяемый дополнительными показателями таблицы 2.

Шаг 7. Оценка динамики рисков нарушения защищенности МСУ в условиях ИТВ состоит в перерасчете функции риска, в которую вводится дополнительный

коэффициент, основанный на распределении Вейбулла-Гнеденко и, в результате, получении динамической оценки защищенности МСУ.

Динамика рисков нарушения защищенности МСУ в условиях ИТВ описывается функцией интенсивности сбоев (отказов), базирующейся на функции распределения Вейбулла-Гнеденко. Функция плотности распределения определена формулой (11), где α – параметр формы распределения, задающий характер динамики риска во время всех стадий жизненного цикла модели (рисунок 2), $R_{БАЗ}$ – параметр, определяющий уровень значения коэффициента базового риска функции распределения

$$f\left(t_{ЖЦ}\right)=\frac{at^{a-1}e^{-\left(\frac{t_{ЖЦ}}{R_{БАЗ}}\right)^{a}}}{R_{БАЗ}}. \qquad (11)$$

Значения функции распределения Вейбулла-Гнеденко сосредоточены на полуоси от 0 до бесконечности. Для экспериментальных исследований динамики рисков нарушения защищенности МСУ в условиях разнотипных и массированных ИТВ и минимизации испытаний введем сдвиговый коэффициент и используем гипотезу о трехпараметрическом распределении Вейбулла-Гнеденко, а также понятие функции риска [4].

Функция динамики оценки рисков нарушения защищенности МСУ выводится из трехпараметрического распределения, результат преобразований приведен в (12). Для получения функции динамики риска нарушения защищенности МСУ $R_{ДИН}(t_{ЖД})$ требуется учет параметра сдвига, определяемого по результатам моделирования и позволяющего построить корректную форму динамики риска для каждого типа МСУ, при этом характер поведения функции определяется (14)

$$R_{\text{ДИН}}\left(t_{\text{ЖЦ}}\right)=\frac{a_k\left(t_{\text{ЖЦ}}-t_k\right)^{(a_k-1)}}{\left(\frac{1}{R_{\text{БАЗ}}}\right)^{a_k}},\ k\in[1,2,3]. \qquad (12)$$

Значения индекса t_k являются различными для разных этапов жизненного цикла модели (рисунок 2), более подробно их формирование описывается в [3]. Общий вид кривой динамики риска будет определяться тремя составляющими модели, для каждой из которых на основе моделирования подбираются свои значения коэффициентов. Базовые условия приведены в (13)

$$a_k:\{k=1:0<a_k<1\{k=2:a_k=1,$$
$$t_k:\{k=1:t_k=0\{k=2:t_k=0, \qquad (13)$$

$$R_{ДИН}\left(t_{ЖЦ}\right):\{a=1:R_{ДИН}(t)=Const\{a>1:R_{ДИН}(t)\uparrow. \qquad (14)$$

Графическое оценивание и прогнозирование изменения функции динамики оценки рисков нарушения защищенности МСУ в условиях ИТВ на основе распределения Вейбула-Гнеденко представлено на рисунке 2.

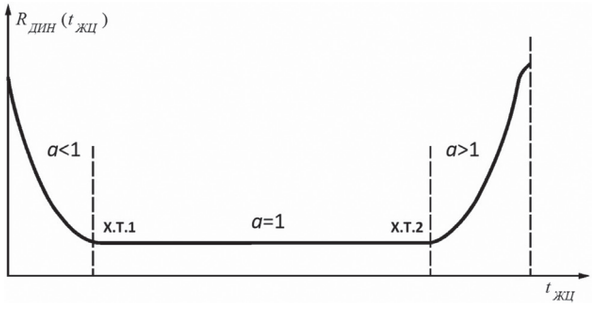

Рисунок 2 – Общий вид функции динамики риска

Динамика риска (первый этап, до характеристической точки х.т.1) определяется повышенным уровнем риска, обусловленным началом эксплуатации системы и следующими потенциальными угрозами:

- сбой (отказ) в работе новой версии программного обеспечения;
- внесенные потенциальные уязвимости в новую версию программного и аппаратного обеспечения;
- недостаточный уровень отладки информационного взаимодействия программных и аппаратных средств МСУ в ходе выполнения ТЦУ.

В то же время уровень риска нарушения защищенности МСУ со временем снижается за счет выпуска и внедрения обновлений программ («патчей») в МСУ, а также доработки алгоритмов управляющих программ с учетом изменений модели угроз ИТВ нарушителя.

На рисунке 2 динамика риска $R_{ДИН}(t_{ЖД})$ на участке между двумя характеристическими точками х.т.1 и х.т.2 (второй этап) является линейной и соответствует базовому уровню риска, полученному на основе статистической оценки (10-12). Этот участок соответствует штатному функционированию отлаженной системы, когда периодичность выхода «патчей» является установившейся величиной и алгоритмы управления МСУ отлажены.

На участке после характеристической точки х.т. 2 (третий этап) $R_{ДИН}(t_{ЖД})$ показывает плавное увеличение уровня риска, что связано как с возможным снижением надежности аппаратных средств, так и появлением со временем не устраненных ошибок в программных средствах, обусловленных ИТВ нулевого дня. Динамическая поправка риска $R_{ДИН}(t_{ЖД})$ (выражение (14)) сформирована таким образом, что на этапе между точками х.т.1 и х.т.2 (второй этап) она имеет значение, равное единице.

Для реальной МСУ требуется уточнение параметров $R_{ДИН}(t_{ЖД})$ с учетом тех особенностей, которыми обладает система и контролируемый сенсорами СОПКА технологический цикл управления. В случае, когда максимально выполнены требования к проектной защищенности МСУ, риск нарушения защищенности будет минимален.

Уточнение значения риска нарушения защищенности будет уточняться по результатам экспериментальных исследований на стендовом полигоне в условиях различных ИТВ, а также с учетом динамики риска на протяжении жизненного цикла системы управления на основе функции риска.

Вывод. Предлагаемая методика оценки защищенности МСУ критически важными информационными объектами позволяет получить числовую статистическую и динамическую оценку риска нарушения защищенности рассматриваемой системы в условиях ИТВ нарушителя. Научная новизна предложенной методики заключается в разработке модели функционирования МСУ в условиях ИТВ на основе расширенных сетей Петри и математических соотношений для определения функции риска нарушения защищенности МСУ с использованием распределения Вейбулла-Гнеденко.

Авторы выражают признательность проф. И.Б. Шубинскому за помощь в оценке интегрального риска нарушения информационной защищенности системы управления.

Библиографический список

1. Климов С.М., Купин С.В., Купин Д.С. Модели вредоносных программ и отказоустойчивости информационно-телекоммуникационных сетей // Надежность. – 2017. – Том 17, № 4. – С. 36-43. DOI: 10.21683/1729-2640-2017-17-4

2. «Умные» среды, «умные» системы, «умные» производства: серия докладов (серия зеленых книг) в рамках проекта «Промышленный и технологический форсайт Российской Федерации» / Коллектив авторов; Фонд «Центр стратегических разработок «Северо-Запад». – СПб, 2012. – Вып. 4. – 62 с.

3. ГОСТ Р 50779.27-2017 Статистические методы. Распределение Вейбулла. Анализ данных.

4. К. Капур, Л. Ламберсон. Надежность и проектирование систем. Под ред. И.А. Ушакова. Пер. с англ. – М.: «Мир», 1980. – 604 с., ил.

5. Климов С.М., Астрахов А.В., Сычев М.П. Методические основы противодействия компьютерным атакам. Электронное учебное издание. – М.: МГТУ имени Н.Э. Баумана, 110 с, 2013.

6. Климов С.М., Астрахов А.В., Сычев М.П. Технологические основы противодействия компьютерным атакам. Электронное учебное издание. – М.: МГТУ имени Н.Э. Баумана, 71 с, 2013.

7. Шубинский И.Б. Надежные отказоустойчивые информационные системы. Методы синтеза / И.Б. Шубинский. – Ульяновск: Областная типография «Печатный двор», 2016. – 544 с.

8. ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем.

9. Климов С.М., Котяшев Н.Н. Метод регулирования рисков комплексов средств автоматизации в условиях компьютерных атак // Надежность. – 2013. – №2. – С. 93-107.

10. Антонов С.Г., Климов С.М. Методика оценки рисков нарушения устойчивости функционирования программно-аппаратных комплексов в условиях информационно-технических воздействий // Надежность. – 2017. – Том 17. – №1. – С.32-39.

11. Климов С.М., Половников А.Ю., Сергеев А.П. Модель функциональной отказоустойчивости процессов обеспечения потребителей навигационными сигналами в сложных условиях // Надежность. – 2017. – Том 17, № 2. – С.41-47.

12. Климов С.М., Поликарпов С.В., Федченко А.В. Методика повышения отказоустойчивости сетей спутниковой связи в условиях информационно-технических воздействий. // Надежность. – 2017. – Том 17, №3. – С. 32-40.

13. Гапанович В.А., Шубинский И.Б., Замышляев А.М. Метод оценки рисков системы из разнотипных элементов // Надежность. – 2016. – Том 16, № 2. – С.49-53.

14. Гапанович В.А., Розенберг Е.Н., Шубинский И.Б. Некоторые положения отказобезопасности и киберзащищенности систем управления // Надежность. – 2014. – №2. – С.88-100.

Сведения об авторах

Сергей М. Климов – доктор технических наук, профессор, начальник управления 4 ЦНИИ Минобороны России, Королев, Россия, e-mail: klimov.serg2012@yandex.ru

Юрий В. Сосновский – кандидат технических наук, доцент кафедры компьютерной инженерии и моделирования Физико-технического института Крымского федерального университета им. В.И. Вернадского, Симферополь, Россия, e-mail:yuri.sosnovskij@yandex.ru

Поступила 23.08.2018