УДК: 629.7 (004.056) DOI: 10.53816/20753608_2022_4_26

МЕТОДИКА СТРУКТУРНО-ПАРАМЕТРИЧЕСКОГО КОНТРОЛЯ И УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ПРИ ВОЗДЕЙСТВИИ ВРЕДОНОСНЫХ ПРОГРАММ

METHODOLOGY FOR STRUCTURAL AND PARAMETRIC CONTROL AND MANAGEMENT OF INFORMATION SECURITY OF CRITICAL INFORMATION INFRASTRUCTURE OBJECTS UNDER THE INFLUENCE OF MALWARE

Академик РАРАН ***В.В. Василенко,*** *чл.-корр. РАРАН* ***С.М. Климов***

4 ЦНИИ МО РФ

V.V. Vasilenko, S.M. Klimov

В статье рассмотрена методика структурно-параметрического контроля и управления информационной безопасностью объектов критической информационной инфраструктуры на основе использования сенсоров обнаружения и нейтрализации вредоносных программ. Информационная безопасность объектов критической информационной инфраструктуры обеспечивается сохранением устойчивости их функционирования в условиях воздействий вредоносных программ. Устойчивость функционирования исследуемых объектов достигается за счет введения в них избыточности — сенсоров обнаружения и нейтрализации вредоносных программ. Сенсоры обеспечивают сбор и обработку статистических данных о событиях информационной безопасности. С использованием этих данных проводится оценка показателей восстанавливаемости, устойчивости и коэффициента готовности.
Ключевые слова: вредоносные программы, объекты критической информационной инфраструктуры, сенсоры обнаружения и нейтрализации вредоносных программ, структурно-параметрический контроль, управление информационной безопасностью.

This article discusses the methodology of the structural and parametric control and management of the information security of the cii facilities based on the use of malware detection and neutralization sensors. The information security of the cii is provided by maintaining. The stability of the functioning of objects is achieved by introducing redundancy into them — maiware detection and neutralization sensors. Sensors provide the collection and processing of information security evend data. These data are used to assess indicators of recoverability, sustainability and readiness coefficients.
Keywords: malware, critical information infrastructure facilities, malware detection and neutralization sensors, structural and parametric control, information security management.

Стратегией национальной безопасности Российской Федерации, утверждённой Указом Президента Российской Федерации от 2 июля 2021 года № 400, определены следующие тенденции нарастания угроз информационной безопасности:

– быстрое развитие информационно-коммуникационных технологий сопровождается повышением вероятности возникновения угроз безопасности граждан, общества и государства;

– увеличивается количество компьютерных атак на российские информационные ресурсы;

– использование в Российской Федерации иностранных информационных технологий и телекоммуникационного оборудования повышает уязвимость российских информационных ресурсов, включая объекты критической информационной инфраструктуры (КИИ) Российской Федерации, к воздействию из-за рубежа.

Для обеспечения информационной безопасности объектов КИИ Российской Федерации необходимо:

– повышать защищённость и устойчивость функционирования объектов КИИ при реализации на них угроз сложных компьютерных атак с использованием вредоносных программ (ВП);

– обнаруживать и нейтрализовывать ВП в объектах КИИ Российской Федерации;

– минимизировать ущерб национальной безопасности, связанный с нарушением информационной безопасности объектов КИИ Российской Федерации;

– совершенствовать методическое обеспечение контроля и управления информационной безопасностью и комплекс средств защиты информации (КСЗИ) на основе применения передовых технологий.

Под ВП нарушителя понимается комплекс программ для организации целенаправленного и скрытного внедрения, создания несанкционированных каналов передачи данных, самораспространения, самомодификации и реализации массированных компьютерных атак на объекты КИИ с целью нарушения устойчивости их функционирования [1, 2]. Возможность воздействия ВП на объекты КИИ обусловлена наличием потенциальных уязвимостей, которые могут использоваться нарушителем для реализации скрытных и целенаправленных информационно-технических воздействий.

Модель процессов функционирования типовых объектов КИИ в условиях ВП нарушителя с использованием моделей [3–5] представлена на рис. 1.

Структура типовых объектов КИИ представлена базовыми элементами, к которым относятся: серверы баз данных (СБД), цифровое коммуникационное оборудование (ЦКО), комплекс средств защиты информации (КСЗИ) и автоматизированные рабочие места (АРМ).

В соответствии с методикой оценки угроз информационной безопасности ФСТЭК России [6], должны учитываться внешние и внутренние угрозы ВП нарушителя.

К внешним угрозам ВП нарушителя следует отнести создание западными странами и террористическими организациями киберподразделений и кибероружия для реализации информационно-технических воздействий на объекты КИИ.

Наличие в объектах КИИ внутренних угроз вызвано, прежде всего, интенсивным внедрением новых информационных технологий, не в полной мере испытанных в условиях воздействия ВП нарушителя, а также «человеческий фактор» в форме некомпетентных и неквалифицированных действий обслуживающего персонала при

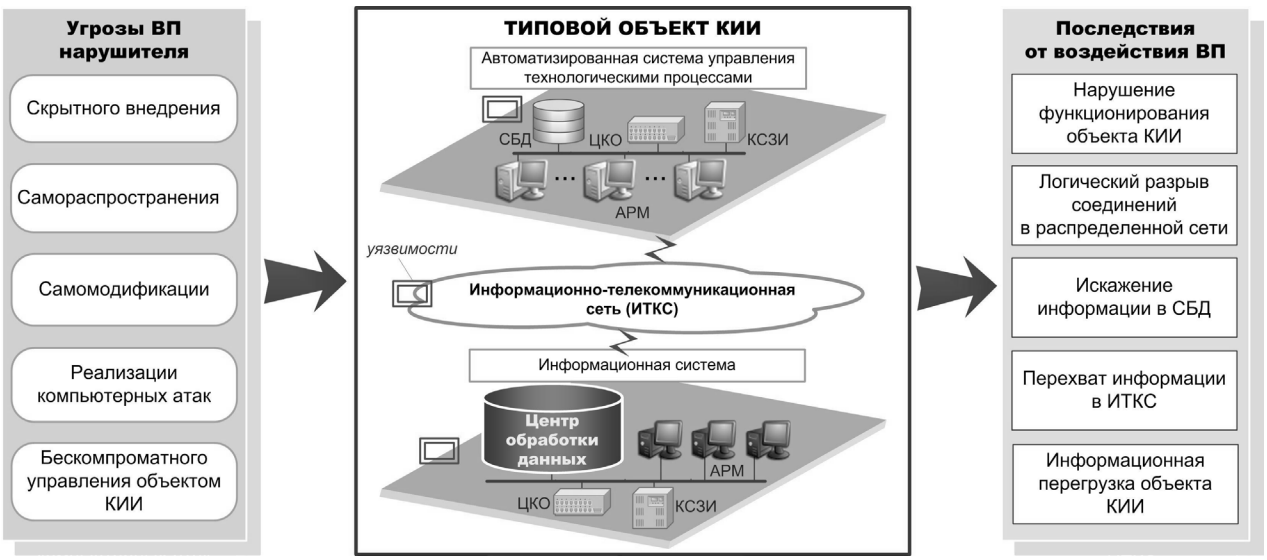

Рис. 1. Модель процессов функционирования типовых объектов КИИ в условиях ВП нарушителя

выполнении организационно-технических мероприятий по обеспечению информационной безопасности объекта КИИ.

Для противодействия ВП нарушителя в сложной и распределенной сети объектов КИИ необходимо разработать методику структурно-параметрического контроля и управления информационной безопасностью объектов КИИ при воздействии ВП, позволяющую проводить мониторинг и обнаружение ВП, управлять информационной безопасностью объектов КИИ на основе оперативной оценки устойчивости функционирования объекта КИИ и динамического выбора вариантов конфигурации КСЗИ.

Существующее методическое обеспечение для противодействия ВП основано, прежде всего, на ручном анализе кода программ, статическом и динамическом анализе программного обеспечения, сигнатурном и поведенческом анализе, а также контроле доступа к файловым системам [7–10].

Модели и методики комплексного обнаружения и количественной оценки характеристик ВП по результатам стендовых испытаний и экспериментальных исследований, выбора вариантов КСЗИ объектов КИИ для противодействия ВП нарушителя недостаточно проработаны.

Актуальность разработки методики структурно-параметрического контроля и управления информационной безопасностью объектов КИИ при воздействии ВП обусловлена [7–10]:

– внедрением новых информационных технологий в объекты КИИ, не в полной мере доверенных по требованиям информационной безопасности и опробованных в условиях применения ВП;

– принятием ведущими зарубежными государствами стратегий кибербезопасности, предусматривающих активные действия в информационном пространстве против других государств;

– сложностью решения задачи повышения устойчивости функционирования объектов КИИ при воздействии ВП существующими методами и КСЗИ;

– необходимостью взаимосвязанного применения организационно-технических мероприятий по обеспечению безопасности информации и КСЗИ для повышения устойчивости функционирования объектов КИИ при воздействии ВП;

– отсутствием отечественных методик комплексного обнаружения, оценки характеристик ВП и выбора необходимых КСЗИ по результатам стендовых испытаний и экспериментальных исследований.

Предполагается, что источником информации при выполнении методики обнаружения и идентификации вредоносных программ в объектах КИИ являются сенсоры обнаружения вредоносных программ (СОВП). Сенсоры представляют собой программно-аппаратные средства, обеспечивающие сбор из системных файлов базовых элементов объекта КИИ данных о событиях безопасности и позволяющие экспериментальным путём получить значения индикаторных параметров признаков ВП.

Схема методики структурно-параметрического контроля и управления информационной безопасностью объектов КИИ при воздействии ВП приведена на рис. 2.

Предложенная схема формализует подход к решению проблемы анализа и синтеза КСЗИ для противодействия угрозам ВП нарушителя на основе разработки методики структурно-параметрического контроля и управления информационной безопасностью объектов КИИ при воздействии ВП.

Сущность структурно-параметрического контроля информационной безопасности объектов КИИ при воздействии ВП состоит в анализе структуры и параметров КСЗИ, необходимых для противодействия угрозам ВП нарушителя, который включает:

– определение потенциальных уязвимостей объектов КИИ при воздействии ВП и оценку их параметров;

– структурно-параметрический контроль событий безопасности, представляющий собой сбор и обработку данных о событиях нарушения информационной безопасности сегментов объектов КИИ, вызванных ВП в соответствии с требованиями стандартов [11–14];

– обнаружение и оценку параметров ВП нарушителя в объектах КИИ на основе применения сенсоров обнаружения вредоносных программ (СОВП);

– разработку требований к структуре и функциям КСЗИ на основе руководящих документов ФСБ России и ФСТЭК России по обеспечению безопасности объектов КИИ при проведении в отношении них компьютерных атак.

На этапе анализа КСЗИ для противодействия угрозам ВП нарушителя должны быть

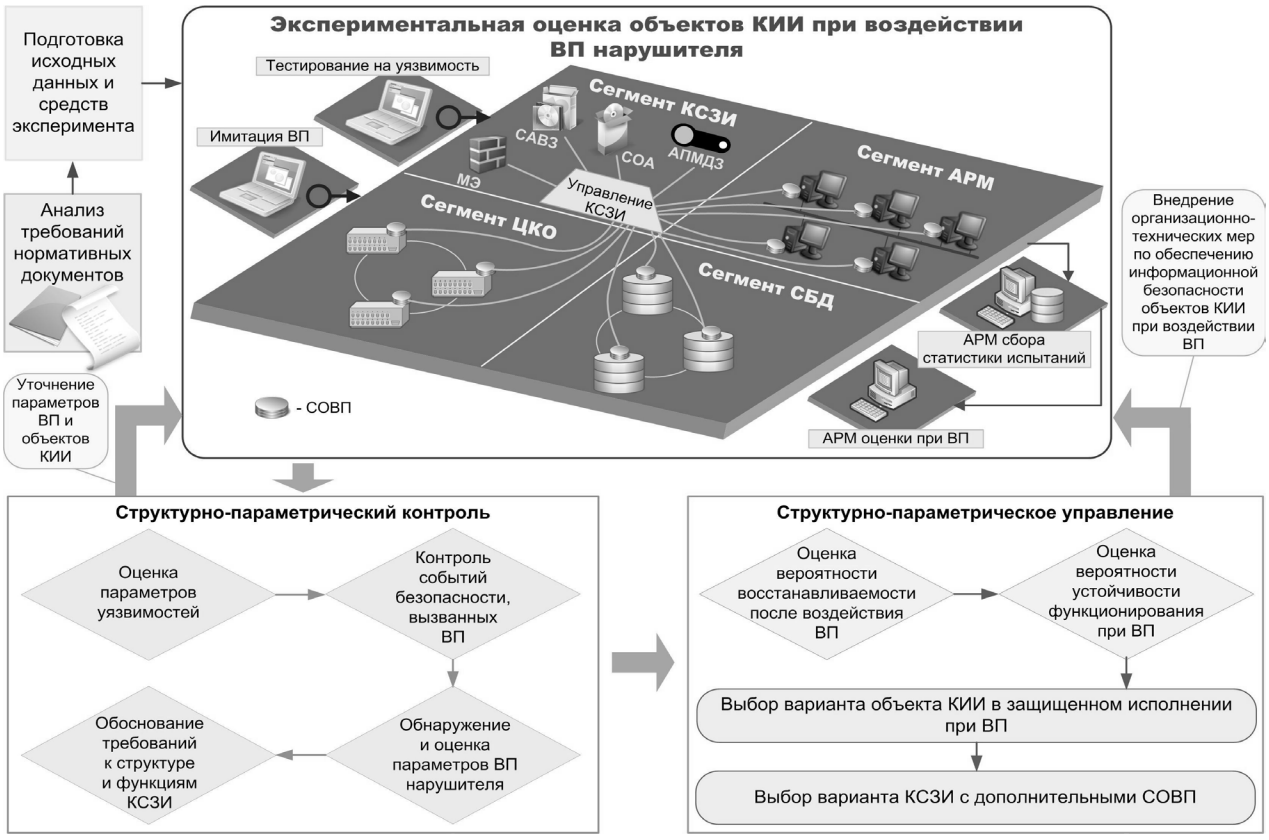

Рис. 2. Схема методики структурно-параметрического контроля и управления информационной безопасностью объектов КИИ при воздействии ВП

разработаны модели и методики для оценки уязвимостей и угроз нарушения информационной безопасности объектов КИИ с учетом особенностей их функционирования [15–18].

С позиций системного подхода структурно-параметрическое управление информационной безопасностью объектов КИИ при воздействии ВП сводится к синтезу КСЗИ и защищенных вариантов объектов КИИ для противодействия угрозам ВП нарушителя, и заключается в следующем:

– оценка показателей восстанавливаемости сегментов объектов КИИ после воздействия ВП;

– оценка устойчивости функционирования сегментов объектов КИИ при ВП;

– выбор вариантов объекта КИИ в защищенном исполнении на основе формирования доверенной операционной среды и типовых регламентов устранения уязвимостей объектов КИИ при воздействии ВП;

– выбор базовых вариантов КСЗИ для противодействия ВП нарушителя с дополнительными СОВП;

– нейтрализация угроз ВП нарушителя на объекты КИИ за счет внедрения дополнительных организационно-технических мер по обеспечению информационной безопасности объектов КИИ при воздействии ВП.

Базовый вариант КСЗИ для противодействия ВП нарушителя на объекты КИИ представляет собой взаимосвязанную совокупность средств защиты информации: межсетевых экранов (МЭ), средств антивирусной защиты (САВЗ), средств обнаружения атак (СОА) и аппаратно-программных модулей доверенной загрузки (АПМДЗ).

В перспективном КСЗИ для объектов КИИ предлагается организовать управление информационной безопасностью путем внедрения в базовые элементы СОВП с функциями не только сбора данных о событиях безопасности, но и управления параметрами КСЗИ и сегментами объекта КИИ.

Структурное управление информационной безопасностью объектов КИИ при воздействии ВП возможно путем выполнения ряда взаимосвязанных процессов:

– блокирование источников ВП по сетевым параметрам на межсетевом экране по данным от СОВП;

– перенаправление сложных компьютерных атак в форме ВП на ложные сетевые информационные объекты;

– реконфигурация распределенной сети объекта КИИ на защищенные подсети;

– организация информационного взаимодействия через криптотуннели и виртуальные частные сети;

– формирование структуры КСЗИ, устойчивых к воздействию ВП нарушителя, на основе многосенсорной технологии применения СОВП.

Дальнейшие исследования по структурно-параметрическому контролю и управлению информационной безопасностью объектов КИИ при воздействии ВП предлагается осуществить в разработке методов определения признаков и деструктивных процессов вредоносных модулей на базе технологий BigData и методов детектирования неизвестных ВП с использованием элементов искусственного интеллекта.

Методика структурно-параметрического контроля и управления информационной безопасностью объектов КИИ при воздействии ВП (рис. 2) основана на многовариантном подходе: введения программной и информационной избыточности, учета параметров угроз ВП, отклонений значений вероятностно-временных показателей объектов КИИ, использования сведений о расследовании компьютерных инцидентов с ВП и устранения уязвимостей.

Под устойчивостью функционирования объекта КИИ понимается его способность выполнять заданные функции на установленном интервале времени с учётом применения КСЗИ и СОВП при воздействии ВП нарушителя [15–18].

Оценка вероятности восстановления объекта КИИ после воздействия ВП на основе комплексного применения КСЗИ и СОВП в период времени восстановления может быть выполнена по формуле:

$$P_{\text{ВОС}}^{\text{КИИ}}\left(t_{\text{ВОС}}\right)=\left\{1-\prod_{i=1}^{N_{\text{КИИ}}}\left[1-e^{-\mu_{\text{КИИ}i}t_{\text{ВОС}}}\right]\right\}\times$$
$$\times\left\{1-\prod_{j=1}^{N_{\text{СОВП}}}\left[1-z_{\text{СОВП}\,j}e^{-\mu_{\text{СОВП}\,j}t_{\text{ВОС}}}\right]\right\}\times$$
$$\times\left\{1-\prod_{m=1}^{N_{\text{КСЗИ}}}\left[1-z_{\text{КСЗИ}m}e^{-\mu_{\text{КСЗИ}m}t_{\text{ВОС}}}\right]\right\},$$

где $t_{\text{ВОС}}$ — время восстановления объекта КИИ; $z_{\text{СОВП}}$, $z_{\text{КСЗИ}}$ — весовые коэффициенты, принимающие значения [0,…,1] и характеризующие количество СОВП и КСЗИ в объекте КИИ, которые обеспечили обнаружение и нейтрализацию ВП; $\mu_{\text{КИИ}}$ — интенсивность восстановления элементов объекта КИИ; $\mu_{\text{СОВП}}$ — интенсивность восстановления объекта КИИ на основе использования компонент СОВП; $\mu_{\text{КСЗИ}}$ — интенсивность восстановления объекта КИИ на основе использования компонент КСЗИ.

Оценка вероятности устойчивости функционирования объекта КИИ при воздействии ВП может быть выполнена по формуле:

$$P_{\text{УСТ}}^{\text{КИИ}}\left(t_{\text{ВП}}\right)=\left[1-\prod_{i=1}^{N_{\text{КИИ}}}P_{\text{ВП}i}\left(t_{\text{ВП}}\right)\right]\times$$
$$\times\prod_{j=1}^{N_{\text{СОВП}}}P_{\text{СОВП}j}(t_{\text{ВП}})\prod_{m=1}^{N_{\text{КСЗИ}}}P_{\text{КСЗИ}m}(t_{\text{ВП}})\times$$
$$\times\prod_{k=1}^{N_{\text{КИИ}}}P_{\text{У}k}(t_{\text{ВП}}),$$

где $t_{\text{ВП}}$ — время воздействия ВП;

$P_{\text{ВП}i}$ — вероятность i-го успешного воздействия ВП на сегменты объекта КИИ, КСЗИ и СОВП;

$N_{\text{КИИ}}$ — количество сегментов в объекте КИИ;

$P_{\text{СОВП}\,j}$ — вероятность обнаружения ВП в j-м элементе СОВП, $j=\{1,...,N_{\text{СОВП}}\}$;

$P_{\text{КСЗИ}m}$ — вероятность нейтрализации ВП m-м элементом КСЗИ, $m=\{1,...,N_{\text{КСЗИ}}\}$;

$P_{\text{У}k}$ — вероятность устранения k-й уязвимости в объекте КИИ, $k=\{1,...,N_{\text{КИИ}}\}$.

Требуемый уровень устойчивости функционирования объекта КИИ при воздействии ВП определяется сохранением им работоспособного состояния на основе обнаружения ВП средствами СОВП, устранения уязвимостей в объекте КИИ и нейтрализации ВП средствами КСЗИ.

Значение требуемого уровня устойчивости функционирования объекта КИИ определяется значением вероятности $P_{\text{УСТ}}^{\text{ТРЕБ}}=0,95$ и задано исходя из опыта по оценке устойчивости объектов КИИ различного целевого назначения [3, 4, 7–9].

Требуемый уровень восстанавливаемости объекта КИИ после воздействия ВП определяет количество СОВП и КСЗИ, которые обеспечили

обнаружение и нейтрализацию ВП за период времени восстановления объекта КИИ.

Выбор варианта объекта КИИ в защищённом исполнении определяется мерами и средствами обеспечения устойчивости функционирования объекта КИИ по границам для максимального и минимального коэффициента готовности [7].

Коэффициент готовности объекта КИИ к выполнению функциональных задач при воздействии ВП определяется соотношением:

$$K_{\Gamma}^{\text{КИИ}} = \frac{t_{\text{КИИ}}}{\sum_{i=1}^{N_{\text{КИИ}}} \left(t_{\text{КИИ}i} + t_{\text{ФО}i}^{\text{ВП}} \right)},$$

где $t_{\text{КИИ}}$ — период времени работоспособного состояния объекта КИИ (до воздействия ВП, приводящего к нарушению функционирования);

$t_{\text{ФО}i}^{\text{ВП}}$ — период функциональных отказов в результате воздействия ВП.

Период времени работоспособного состояния одного сегмента объекта КИИ определим выражением:

$$t_{\text{КИИ}} = \frac{1}{N_{\text{КИИ}} \mu_{\text{КИИ}} \mu_{\text{СОВП}} \mu_{\text{КСЗИ}}}.$$

Период функционального отказа одного сегмента объекта КИИ в результате воздействия ВП запишем в виде:

$$t_{\text{ФО}}^{\text{ВП}} = \frac{1}{N_{\text{КИИ}} \lambda_{\text{ВП}} \left(1 - P_{\text{АД}}\right)},$$

где $\lambda_{\text{ВП}}$ — интенсивность воздействия ВП;

$P_{\text{АД}}$ — вероятность успешной адаптации объекта КИИ с основными резервируемыми базовыми элементами ЦКО, КСЗИ, СБД и АРМ к воздействию ВП.

Вероятность успешной адаптации сегментов объекта КИИ характеризует своевременность обнаружения функционального отказа, вызванного воздействием ВП, и устранением его путем оперативного восстановления отказываемого сегмента или подключения резервного сегмента.

Границы для максимального и минимального коэффициента готовности объекта КИИ с учетом [7] определим исходя из следующих предположений:

– период времени функциональных отказов (минимального значения неработоспособности объекта КИИ) в результате воздействия ВП соответствует периоду среднего времени восстановления объекта КИИ;

– основные и резервные элементы объекта КИИ (ЦКО, КСЗИ, СБД, АРМ и СОВП) однотипны, и время их восстановления после воздействия ВП одинаково;

– средства КСЗИ и СОВП обеспечивают адаптацию процессов функционирования СБД и АРМ к условиям воздействия ВП и их восстановление;

– готовность объекта КИИ к условиям воздействия ВП зависит от вероятности и своевременности обнаружения и нейтрализации этих воздействий средствами КСЗИ и СОВП.

Граница для максимального коэффициента готовности сегмента к выполнению функциональных задач при воздействии ВП:

$$K_{\Gamma\max}^{\text{КИИ}} \le \frac{1}{1 + N_{\text{КИИ}} \lambda_{\text{ВП}} \left(1 - P_{\text{АД}}\right)}. \qquad (1)$$

Граница для минимального коэффициента готовности объекта КИИ к выполнению функциональных задач при воздействии ВП:

$$K_{\Gamma\min}^{\text{КИИ}} \ge 1 - K_{\Gamma\max}^{\text{КИИ}}. \qquad (2)$$

Тогда, подставляя в (2) значение $K_{\Gamma\max}^{\text{КИИ}}$ из (1), получим выражение:

$$K_{\Gamma\min}^{\text{КИИ}} \ge \frac{N_{\text{КИИ}} \lambda_{\text{ВП}} \left(1 - P_{\text{АД}}\right)}{1 + N_{\text{КИИ}} \lambda_{\text{ВП}} \left(1 - P_{\text{АД}}\right)}.$$

Повышение коэффициента готовности достигается при обеспечении вероятности успешной адаптации сегмента к отказам $P_{\text{АД}}$ на уровне большем 0,85–0,90.

Требуемые значения коэффициента готовности объекта КИИ при реализации ВП находятся между максимальными и минимальными его значениями.

Таким образом, разработана методика структурно-параметрического контроля и управления информационной безопасностью объектов КИИ при воздействии ВП, которая основана на учёте угроз ВП и последствий от их воздействия, внедрении СОВП, анализе и синтезе КСЗИ и защищенных вариантов объектов КИИ для противодействия угрозам ВП, определении показателей восстанавливаемости

и устойчивости функционирования объекта КИИ, а также на выборе рационального варианта мер и средств обеспечения устойчивости функционирования объекта КИИ по границам для максимального и минимального коэффициента готовности.

Литература

1. Монаппа К.А. Анализ вредоносных программ / пер. с анг. Д.А. Беликова. — М.: ДМК Пресс, 2019. 452 с.: ил.

2. Антонов С.Г. и др. Модели выявления уязвимостей в автоматизированных информационных системах и анализ угроз информационно-технических воздействий // Труды XXIII Всероссийской научно-практической конференции «Актуальные проблемы защиты и безопасности». 2020. Т. 3. С. 8–15.

3. Климов С.М. Методы и модели противодействия компьютерным атакам. — Люберцы: Изд-во КАТАЛИТ, 2008. 316 с.

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

5. Купин С.В., Купин Д.С. и др. Модели вредоносных программ и отказоустойчивости информационно-телекоммуникационных сетей // Надежность. 2017. № 4. С. 36–43.

6. Методика оценки угроз безопасности информации. ФСТЭК России. 2021. 83 с.

7. Шубинский И.Б. Надежные отказоустойчивые информационные системы. Методы синтеза / И.Б. Шубинский. — Ульяновск: областная типография «Печатный двор». 2016. 544 с.: ил.

8. Шубинский И.Б. Функциональная надежность информационных систем. Методы анализа. — Ульяновск: областная типография «Печатный двор», 2012. 296 с.: ил.

9. Шубинский И.Б. Структурная надежность информационных систем. Методы анализа. — Ульяновск: областная типография «Печатный двор», 2012. 216 с.: ил.

10. Поликарпов С.В., Рыжов Б.С., Тихонов Р.И. и др. Методика обеспечения устойчивости функционирования критической информационной инфраструктуры в условиях информационных воздействий // Журнал «Вопросы кибербезопасности». 2019. № 6 (34). 2019. С. 37–48.

11. ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. — М.: Стандартинфор, 2018. 8 с.

12. ГОСТ Р 56545-2015 Защита информации. Уязвимости информационных систем. Правила описания уязвимостей. — М.: Стандартинфор, 2018. 8 с.

13. ГОСТ Р 59547-2021 Защита информации. Мониторинг информационной безопасности. Общие положения. — М.: Российский институт стандартизации, 2021. 15 с.

14. ГОСТ Р 59548-2022. Защита информации. Регистрация событий безопасности. Требования к регистрации информации, которые определяют требования и порядок регистрации событий информационной безопасности в интересах ликвидации последствий ИТВ и реагирования на компьютерные инциденты. — М.: Российский институт стандартизации, 2021. 70 с.

15. Антонов С.Г., Анциферов И.И. и др. Методика расчетно-экспериментальной оценки устойчивости объектов критической информационной инфраструктуры при информационно-технических воздействиях // Надежность. 2020. Том 20. № 4. С. 34–41.

16. Ерохин С.Д., Петухов А.Н., Пилюгин П.Л. Управление безопасностью критических информационных инфраструктур. — М.: Горячая линия — Телеком, 2021. 240 с.:ил.

17. Василенко В.В., Гвоздева Г.А., Купин С.В. и др. Методика обнаружения и оценки вредоносных программ в объектах критической информационной инфраструктуры // Труды XXV Всероссийской научно-практической конференции «Актуальные проблемы защиты и безопасности». 2022. Т. 3. С. 116–123.

18. Василенко В.В., Гвоздева Г.А., Палухин О.А. и др. Методика экспериментальной оценки функциональной устойчивости системы обнаружения и предупреждения компьютерных атак сетей электросвязи // Военная безопасность России: взгляд в будущее. Материалы 7-й Международной межведомственной научно-практической конференции научного отделения № 10 РАРАН. 2022. Т. 1. С. 202–206.