МЕТОДИКА ОБЕСПЕЧЕНИЯ УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ В УСЛОВИЯХ ИНФОРМАЦИОННЫХ ВОЗДЕЙСТВИЙ

Климов С.М.¹, Поликарпов С.В.², Рыжов Б.С.³, Тихонов Р.И.⁴, Шпырня И.В.⁵

Аннотация. Целью статьи является разработка методики, которая позволяет определить вероятностно-временные показатели обеспечения устойчивости функционирования критической информационной инфраструктуры в условиях информационных воздействий. К информационным воздействиям относится совокупность информационно-технических и информационно-психологических воздействий. В критической информационной инфраструктуре рассматриваются уязвимости информационно-телекоммуникационных сетей, автоматизированных систем управления технологическими процессами и информационных систем к информационно-техническим воздействиям, а также уязвимость «человека-оператора» к информационно-психологическим воздействиям. Элементы критической информационной инфраструктуры являются «человеко-машинными» взаимосвязанными системами, в которых информационное воздействие на оператора и/или компьютеризированные средства приводит к снижению эффективности критической информационной инфраструктуры в целом.

В качестве информационно-технических воздействий рассматриваются целенаправленные программные воздействия на программы и информацию критической информационной инфраструктуры с целью временного нарушения процессов ее функционирования. Информационно-психологическое воздействие – воздействие на операторов и население в местах размещения критической информационной инфраструктуры через социальные сети, электронные средства массовой информации, мобильные приложения и другие ресурсы сети Интернет, приводящее к дестабилизации обстановки, срыву регламентов работы и снижению устойчивости функционирования критической информационной инфраструктуры. Осуществление угроз совместных информационно-технических и информационно-психологических воздействий возможно при наличии уязвимостей в критической информационной инфраструктуре и доступности Интернет-ресурсов для операторов и населения в районах эксплуатации критической информационной инфраструктуры.

Методика основана на следующих допущениях: оценка вероятностно-временных показателей критической информационной инфраструктуры осуществляется по результатам экспериментальных исследований на киберполигоне; существуют имитаторы информационных воздействий; обеспечение устойчивости функционирования реализуется за счет структурно-функциональной избыточности; разработаны типовые сенсоры обнаружения, предупреждения и ликвидации последствий информационных воздействий; реагирование на компьютерные инциденты осуществляется за счет восстановления работоспособности системы.

В рамках методики разработаны вероятностно-временные показатели обеспечения устойчивости критической информационной инфраструктуры при реализации информационно-технических воздействий и оценки рисков информационно-психологических воздействий на операторов и населения в местах размещения элементов инфраструктуры.

Ключевые слова: вероятностно-временные показатели, информационно-технические воздействия, информационно-психологические воздействия, сенсоры информационных воздействий, уязвимости, риски нарушения устойчивости функционирования, средства защиты информации.

DOI: 10.21681/2311-3456-2019-6-37-48

1 Климов Сергей Михайлович, доктор технических наук, профессор, сотрудник 4 ЦНИИ Минобороны России, Королёв. Россия. E-mail: klimov.serg2012@yandex.ru

2 Поликарпов Сергей Викторович, сотрудник 4 ЦНИИ Минобороны России, Королёв. Россия. E-mail: polikarpov.s.v@yandex.ru

3 Рыжов Борис Сергеевич, кандидат технических наук, доцент, сотрудник 4 ЦНИИ Минобороны России, Королёв. Россия. E-mail: ryzhov5@ya.ru

4 Тихонов Рудольф Игоревич, сотрудник 4 ЦНИИ Минобороны России, Королёв. Россия. E-mail: tihonovrudolf@mail.ru

5 Шпырня Игорь Валентинович, сотрудник Восьмого Управления Генерального штаба ВС РФ, Москва. Россия. E-mail: z@mil.ru

Введение

Стратегия развития информационного общества предполагает интенсивное внедрение в критическую информационную инфраструктуру (КИИ) отечественных и зарубежных информационных и коммуникационных технологий.

Внедрение указанных технологий предполагает использование значительных объемов данных, множества стеков протоколов передачи данных (например, более 200 стеков протоколов передачи данных типа TCP/IP) для организации обработки информации и взаимосвязанного информационного обмена в режиме удаленного доступа между объектами и субъектами КИИ. Известно, что с увеличением объема программного обеспечения по экспоненциальной зависимости возрастает число ошибок в нем, которые и являются уязвимостями для информационных воздействий [1].

Человек-оператор как неотъемлемая часть элементов КИИ в процессе выполнения служебных обязанностей и вне рабочее время в рамках своей целевой аудитории также является уязвимым для информационно-психологических воздействий с использованием Интернет технологий (социальных сетей, электронных средств массовой информации, мобильных приложений и других Интернет-ресурсов) [2].

Критическая информационная инфраструктура дала толчок для развития нового информационного общества и цифровой экономики, но одновременно, стало ожесточенной ареной противостояния государств и ведения гибридных войн [3].

Наличие множества уязвимостей в КИИ создает предпосылки для реализации потенциальных угроз целенаправленных и массированных информационно-технических воздействий (ИТВ) и информационно-психологических воздействий (ИПВ), приводящих к компьютерным инцидентам в КИИ [4].

Под ИТВ понимаются целенаправленные и взаимосвязанные программно-аппаратные и программные воздействия, приводящие к нарушению функционирования, снижению эффективности выполнения технологических циклов управления или логическому выводу из строя КИИ. Как правило, информационно-технические воздействия осуществляются в форме несанкционированного доступа к информационным ресурсам КИИ, распределенных компьютерных атак (DDoS-атак), скрытого проникновения вредоносной программной информации, инициализации программно-аппаратных закладок (недекларированных возможностей) и информационной нагрузки [5].

К факторам ИПВ относятся воздействия на операторов, членов их семей и целевую аудиторию в местах размещения КИИ с использованием ресурсов сети Интернет, приводящие к деморализации операторов, дестабилизации обстановки, срыву регламентов работы и потере управляемости элементами КИИ [6]. Последствием реализации угроз информационных воздействий (компьютерных атак) является нарушение устойчивости функционирования элементов КИИ [7].

Целью выполнения требований к безопасности КИИ – обеспечение устойчивого функционирования КИИ при проведении в отношении ее ИТВ и ИПВ.

Поэтому разработка методики, позволяющей определить вероятностно-временные показатели обеспечения устойчивости функционирования КИИ при реализации комплексных угроз ИТВ и ИПВ, является актуальной.

Постановка задачи

В настоящее время КИИ представляет собой совокупность информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, а также сетей электросвязи, используемых для взаимодействия объектов КИИ.

В статье рассмотрены: уязвимости КИИ, классификация угроз ИТВ и ИПВ, методические положения по нейтрализации этих угроз на основе комплекса мер по обеспечению защищенности и устойчивости функционирования объектов и субъектов КИИ от чрезвычайных ситуаций, вызванных этими воздействиями.

Йоттабайты (10^{24} байт) цифровых данных и компьютерных программ необходимы для выполнения сложных и опасных технологических процессов в системах энергетики, финансовых системах, системах управления транспортом и городской инфраструктурой, производством, системах связи и навигации ведущих стран мира. Они становятся объектами нарушения безопасности информации КИИ, а как следствие нарушение устойчивости ее функционирования [8].

Интенсивное внедрение информационных и коммуникационных технологий в КИИ с использованием зарубежного программного кода увеличивает уязвимости, через которые могут быть реализованы целенаправленные компьютерные атаки, наносящие значительный ущерб объектам инфраструктуры [9].

Наибольшую уязвимость в КИИ вносят операционные системы и общедоступные протоколы передачи данных типа TCP/IP, используемые в глобальной сети Интернет, а также различные сетевые сервисы. Практически все элементы автоматизированных систем управления производственными процессами (так называемые SCADA-системы) являются IP-устройствами, работающими в режиме удаленного доступа [10]. Так, например, статистика «Лаборатории Касперского» по компьютерным атакам вредоносного типа показывает, что в первом полугодии 2018 года в системах промышленной автоматизации было обнаружено более 19,4 тысяч модификаций вредоносных программ [11].

Наиболее популярными источниками информации, размещаемой в сети Интернет, являются социальные сети и информационные ресурсы Одноклассники, Facebook, Twitter, Instagram и ВКонтакте, с использованием которых могут быть реализованы ИПВ на целевую аудиторию операторов КИИ [12].

С использованием методов обеспечения надежности и устойчивости функционирования сложных технических систем [13] методику обеспечения устойчивости функционирования КИИ в условиях информационных воздействий (рис.1) представим следующей последовательностью шагов:

1. Анализ совместных угроз ИТВ и ИПВ и выявление уязвимостей в КИИ.

- Выбор (разработка) средств обеспечения устойчивости функционирования КИИ в условиях угроз комплексных ИТВ и ИПВ (сенсоров средств обнаружения, предупреждения и ликвидации последствий компьютерных атак в форме ИТВ (СОПКА-ИТВ) и в форме ИПВ (СОПКА-ИПВ), вариантов комплексов средств защиты информации (КСрЗИ) от ИТВ и ИПВ) [14].
- Проведение экспериментальных исследований с элементами КИИ в условиях информационных угроз на киберполигоне.
- Оценка вероятностно-временных показателей обеспечения устойчивости программно-технических элементов (ПТЭ) КИИ при реализации ИТВ.
- Оценка рисков успешных ИПВ на операторов и население в местах размещения элементов КИИ.

[15]. Кроме того, уязвимыми являются параметры синхронизации и сигнализации в магистральных каналах связи с программируемой маршрутизацией. В настоящее время в России наиболее широко используются базы данных угроз и уязвимостей программного обеспечения ФСТЭК России – BDU и международная классификация – CVE.

Уязвимостями к ИПВ целевой аудитории операторов КИИ, использующей информационные ресурсы сети Интернет, являются API (интерфейс взаимодействия между сайтом и сторонними программами и сервером), URL-адрес (адрес сайта в сети Интернет), IP и MAC адреса операторов в сети Интернет вне контролируемой зоны КИИ, DNS-сервер, аккаунт и контент оператора в сети Интернет [16].

Рис.1. Схема методики обеспечения устойчивости функционирования КИИ в условиях ИТВ и ИПВ

Шаг 1. Анализ уязвимостей в КИИ и совместных угроз ИТВ и ИПВ.

К уязвимостям КИИ относятся программные, архитектурные или логические недостатки в КИИ, используя которые возможно получить несанкционированный доступ к защищаемой информации, нарушить ее целостность и доступность, а также вызвать нарушение функционирования КИИ. К основным уязвимостям распределенных сетей КИИ к ИТВ относятся недостаточная защищенность протоколов, слабая идентификация (аутентификация), MAC-адрес, IP-адрес, логическое имя абонента сети, номера портов, наличие большого количества точек доступа для организации маршрутизации потоков данных и логики взаимодействия абонентов

Наибольшую опасность представляют целенаправленные (таргетированные) атаки и ИТВ вредоносного типа (рис.2). В практике компьютерных инцидентов известны самораспространяющиеся по принципу эпидемий вредоносные программы, такие как Stuxnet, Flame, Duqu, Gauss, Reign, Wiper, Shamoan [17].

Указанные программы реализованы на основе кросс-платформенной технологии, скрытно внедряют свой код в систему, распространяются с учетом специфики технологических циклов управления системы, собирают информацию о ней, развертывают атакующую сеть (до десятков тысяч компьютеров в глобальной сети), и по команде, реализуют массовые сбои и отказы в элементах КИИ [18].

Информационно-психологические воздействия могут осуществляться на операторов и население в местах размещения КИИ через социальные сети, электронные средства массовой информации, мобильные приложения и другие ресурсы сети Интернет. Последствия этих воздействий заключаются в дестабилизации обстановки, срыве регламентов работы и снижении эффективности функционирования КИИ.

1. Отдельные и групповые ИТВ самостоятельно реализующие деструктивные функции на КИИ (например, для нанесения экономического ущерба КИИ).
2. ИТВ, используемые для доставки ИПВ в интересах манипулирования целевой аудиторией КИИ.
3. ИПВ самостоятельно реализующие функции воздействия на целевую аудиторию КИИ (фальсификация, дезинформация, дискредитация).

Рис.2. Классификация ИТВ по возможным каналам доступа и последствиям нарушения вычислительных процессов в КИИ

Опасность реализации ИПВ на операторов и население в местах размещения КИИ обусловлена тем, что даже существенно компьютеризированные и роботизированные системы являются «человеко-машинными» системами, в которых задачи управления и принятия решений выполняет «человек-оператор». «Человек-оператор» и является потенциально уязвимым человеческим компьютерным фактором для воздействия ИПВ как в рабочей, так и домашней обстановке [19].

Предполагается, что нарушителем объединяются возможности ИТВ и ИПВ в рамках сценария таргетированных (целевых и спланированных) воздействий на объекты и субъекты КИИ.

Особо уязвимы для реализации совместных ИТВ и ИПВ информационные ресурсы КИИ, подключенные к сети Интернет. Даже при наличии средств защиты информации в таких системах всегда существуют потенциальные неизвестные угрозы ИТВ и ИПВ «нулевого» дня (не идентифицированные и не имеющие средств защиты информации на момент воздействия).

Варианты реализации угроз комплексных ИТВ и ИПВ на КИИ следующие:

4. ИПВ для «тандемного» усиления ущерба от ИТВ (например, выдвижение экономических требований или оплаты за восстановление компьютерной сети, банковской системы после ИТВ).
5. ИТВ применяемые совместно с ИПВ для информационной блокады, изоляции регионов и акваторий размещения КИИ, нарушения КИИ и дальнейшей дестабилизации обстановки.

Шаг 2. Выбор (разработка) средств обеспечения устойчивости функционирования КИИ в условиях угроз комплексных ИТВ и ИПВ осуществляется на базе сенсоров СОПКА-ИТВ и СОПКА-ИПВ, вариантов комплекса средств защиты информации (КСрЗИ) от ИТВ и ИПВ (рис. 3).

Сущность схемы обеспечения устойчивости функционирования КИИ в условиях угроз комплексных ИТВ и ИПВ заключается в том, что элементы КИИ являются «человеко-машинными» взаимосвязанными системами, в которых информационное воздействие на человека и/или компьютеризированные, роботизированные средства приводит к снижению эффективности КИИ в целом.

Рис.3. Схема обеспечения устойчивости функционирования КИИ в условиях угроз комплексных ИТВ и ИПВ

Обеспечение устойчивого функционирования КИИ предлагается осуществить по двум основным направлениям:

1. Реализация СОПКА-ИТВ.
2. Реализация СОПКА-ИПВ.

По первому направлению необходимо развернуть центры мониторинга КИИ для нейтрализации ИТВ с привлечением ведущих производителей средств обнаружения вторжений и реагирования на компьютерные инциденты [20].

По второму направлению предлагается создать комплексы мониторинга и оценки информационной обстановки в местах эксплуатации КИИ.

Базовыми элементами СОПКА-ИТВ предлагается сделать следующие виды сенсоров: каналов управления, каналов передачи данных, полезной нагрузки, магистральных сетей электросвязи, информационно-вычислительных процессов, навигационных сигналов.

Сенсоры представляют собой программные или программно-аппаратные средства обнаруживающие ИТВ на основе детерминированных методов сигнатурного анализа и анализа аномалий эвристическими методами.

По аналогии с СОПКА-ИТВ базовыми элементами (СОПКА-ИПВ) предлагается сделать следующие виды сенсоров: текстовой информации, графической и видеоинформации, картографической информации, звуковой информации.

Сенсоры представляют собой программные или программно-аппаратные средства обнаруживающие ИПВ с использованием лингвистического анализа дан-

ных, нейронных сетей и технического анализа информации в сегментах сети Интернет объектов КИИ. Сенсорами обнаружения ИПВ информация в сети Интернет может разделяться на негативную, нейтральную и позитивную, а также декомпозироваться на более точные тональности ее оценки.

Два контура средств СОПКА-ИТВ и СОПКА-ИПВ позволяют обнаружить информационные воздействия, идентифицировать их и собрать необходимую информацию в унифицированном формате. Кроме того, должны быть предусмотрены средства принятия решений по компьютерным инцидентам в КИИ для восстановления ее работоспособности и переключения на резервные системы.

Шаг 3. Проведение экспериментальных исследований с элементами КИИ в условиях информационных угроз на киберполигоне необходимо для получения статистики по параметрам уязвимостей КИИ, угроз ИТВ и ИПВ, КСрЗИ (средства обнаружения вторжений, межсетевые экраны, средства антивирусной защиты, средства защиты от не санкционированного доступа).

Для априорной оценки функциональных возможностей КИИ и соответствующих КСрЗИ, отработки действий операторов СОПКА-ИТВ и СОПКА-ИПВ предлагается проводить экспериментальные исследования на киберполигоне и мероприятия по оценке реальной защищенности элементов КИИ в условиях информационных воздействий.

Шаг 4. Оценка вероятностно-временных показателей обеспечения устойчивости программно-технических элементов (ПТЭ) КИИ при реализации ИТВ с ис-

пользованием экспериментальных данных полученных на киберполигоне включает определение следующих показателей:

- верхних и нижних оценок вероятностей связности графа элементов и сенсоров ПТЭ КИИ,
- вероятности невыполнения технологического цикла управления (ТЦУ) ПТЭ в условиях ИТВ с необходимой интенсивностью передачи данных λ .

Верхние и нижние оценки вероятностей связности графа элементов и сенсоров ПТЭ КИИ получим с использованием метода Литвака-Ушакова, использующего структурные функции графа для минимальных путей и разрезов (последовательно-параллельных соединений) двухполюсного графа [21] следующим образом:

1. Определение структурных функций схем применения элементов и сенсоров ПТЭ КИИ:

а) структурная функция минимальных путей в графе:

$$F_{\Pi}(S) = \bigcup_{1 \leq j \leq N} h_j(S), \quad h_j(S) = \bigcap_{i \in A_j} S_i, \quad (1)$$

где: $S = (S_1, S_2, \dots, S_i)$ – i -мерный вектор состояний ПТЭ в виде связанного графа, $h_j(S)$ – минимальный путь в графе, A_j – подмножество рёбер графа, образующих j -й минимальный путь,

$$F_{\Pi}(S) = \begin{cases} 1, & \text{если состояние (S) СУПД соответствует устойчивому функционированию;} \\ 0, & \text{если нарушено (прекращено) функционирование;} \end{cases}$$

б) структурная функция минимальных разрезов в графе:

$$F_p(S) = \bigcap_{1 \leq k \leq M} d_k(S), \quad d_k(S) = \bigcup_{i \in B_k} S_i, \quad (2)$$

где: $d_k(S)$ – минимальный разрез в графе, B_k – подмножество рёбер графа, образующих k -й минимальный разрез,

$$F_p(S) = \begin{cases} 1, & \text{если состояние (S) СУПД соответствует устойчивому функционированию;} \\ 0, & \text{если нарушено (прекращено) функционирование.} \end{cases}$$

2. Выбор мостиковых схем осуществляется с использованием минимальных путей и разрезов графа состояний элементов и сенсоров ПТЭ КИИ (рис. 4).

Рис. 4. Типовые схемы для выделения минимального разреза графа состояний (для верхней оценки) и минимального пути графа состояний (для нижней оценки)

3. Вычисление верхних и нижних оценок вероятностей связности графа элементов и сенсоров ПТЭ КИИ:

а) верхняя оценка вероятностей связности:

$$\bar{H}_{\Pi}^H = \min_{1 \leq m \leq M} \prod_{1 \leq k \leq N_m} \left[1 - \prod_{i \in B_k^m} q_i \right], \quad (3)$$

где q_i – вероятность повышения устойчивости функционирования ПТЭ КИИ за счёт высоконнадёжных элементов;

б) нижняя оценка вероятностей связности:

$$\bar{H}_{\Pi}^B = \max_{1 \leq l \leq L} \left[1 - \prod_{1 \leq j \leq U_l} \left(1 - \prod_{i \in A_j^l} r_i \right) \right], \quad (4)$$

где $r_i = 1 - q_i$ – вероятность нарушения функционирования ПТЭ КИИ из-за ненадёжных элементов.

4. Получение наилучшей верхней оценки вероятности связности графа состояний ПТЭ КИИ:

$$\bar{H}_{ЛВ}^H \leq MF(S) \leq \bar{H}_{ЛВ}^B. \quad (5)$$

Определение вероятности не выполнения ТЦУ ПТЭ в условиях ИТВ с необходимой интенсивностью передачи данных λ с применением метода Эрланга [22]:

а) функция распределения нахождения ПТЭ в работоспособном состоянии:

$$f_p(t) = \sum_{j=1}^k p_j \cdot c_j \cdot t^{m_j-1} \cdot e^{-\lambda_j m_j t}, \quad t \geq 0, \quad \sum_{j=1}^k p_j = 1, \quad (6)$$

где: p_j - вероятность нахождения ПТЭ в работоспособном состоянии, $c_j = (\lambda_j n_j)^{n_j} / (n_j - 1)!$, t - период времени выполнения ТЦУ ПТЭ, m_j - вспомо-

гательные состояния для расщепления работоспособного состояния ПТЭ, λ_j - интенсивность передачи данных ПТЭ и ИТВ;

б) функция распределения нахождения ПТЭ в состоянии отказа:

$$f_{отк}(t) = \sum_{i=1}^k g_i \cdot d_i \cdot t^{n_i-1} e^{-\mu_i n_i t}, \quad t \geq 0, \quad \sum_{i=1}^k g_i = 1, \quad (7)$$

где: g_i - вероятность нахождения ПТЭ в состоянии отказа, $d_i = (\mu_i n_i)^{n_i} / (n_i - 1)!$, μ_i - интенсивность потока заявки на восстановление ПТЭ, n_i - вспомогательные состояния для расщепления состояния отказа ПТЭ.

Определение функции распределения случайного времени пребывания ПТЭ в состояниях работоспособности и отказов в виде последовательности из m сто-

хастически независимых временных фаз случайной длительности (рис. 5), где каждая фаза распределена с параметром μ_i осуществляется с использованием выражений:

$$f_{p,j}(t) = c_j \cdot t^{m_j-1} \cdot e^{-\lambda_j m_j t}, \quad (8)$$

$$t \geq 0, \quad f_{отк,i}(t) = d_i \cdot t^{n_i-1} e^{-\mu_i n_i t}, \quad t \geq 0.$$

Вероятность невыполнения ТЦУ CCC с необходимой интенсивностью передачи данных λ :

$$P_{нвост}(t) = \int_{t_0}^{t_0 + \Delta t} f_{отк}(t) dt \quad (9)$$

По эмпирически полученным данным о времени пребывания ПТЭ в фазах состояния отказов, восстановления, работоспособности и реализации ИТВ с применением метода Эрланга осуществляется расщепление состояний на фиктивные состояния. При этом распределение Эрланга можно рассматривать как распределение суммы независимых, экспоненциально распределенных с параметрами и случайных величин. Введение дополнительных состояний позволяет описать систему с помощью однородного Марковского процесса.

Шаг 5. Оценка рисков успешных ИПВ на операторов и население в местах размещения элементов КИИ (рис. 6).

Модель угроз ИПВ на операторов и членов их семей в местах размещения КИИ объединяет следующие компоненты [23]:

угрозы ИПВ, которые проиндексированы по возможным их способам реализации (Y1 - Y8),

степень влияния угроз ИПВ, которая характеризуется интенсивностью ИПВ (частота реализации ИПВ на недельном интервале от 10-1 до 10-9), вероятностью успешности их реализации (определяется величинами от 0 до 1) и величиной ущерба (измеряется от 1 до 10 и определяется экспертным путем),

четырёхуровневую оценку рисков снижения эффективности применения КИИ.

Рис.5. Схема графа переходов сегментов CCC между работоспособными состояниями и состояниями отказов с применением метода фаз Эрланга

Рис.6. Модель угроз ИПВ на КИИ с использованием сети Интернет

Четырехуровневая оценка рисков нарушения устойчивости функционирования КИИ в условиях ИПВ необходима для оценки чрезвычайных ситуаций, вызванных информационными воздействиями на КИИ и базируется на принципе ALARP риск нарушения функционирования КИИ можно уменьшить настолько насколько это достижимо на практике [24].

Оператор рассматривается как один из элементов «человеко-машинных» ПТЭ КИИ, функционирование которых может быть нарушено в условиях ИПВ. Предполагается, что процессы реализации ИПВ являются независимыми и распределены по экспоненциальному закону. Успешные ИПВ приводят к риску возникновения сбоев и отказов КИИ.

Оценка вероятности успешных ИПВ на операторов и население в местах размещения элементов КИИ в определяется с учетом интенсивности успешных ИПВ $\lambda_{ИПВ_i}$:

$$P_{ИПВ_i}(t_{ИПВ_i}) = \prod_{i=1}^k (1 - e^{-\lambda_{ИПВ_i} t_{ИПВ_i}}), \quad (10)$$

где $\lambda_{ИПВ_i}$ – среднее число успешно реализованных

ИПВ в единицу времени, i – вариант ПТЭ КИИ, $t_{ИПВ_i}$ – длительность воздействия ИПВ.

Критерии для оценки влияния ИПВ на устойчивость функционирования КИИ определяется путем оценки уровня допустимого риска нарушения устойчивости функционирования КИИ по принципу ALARP на основе модели на (рис. 6) и (табл. 1).

Область ALARP риска нарушения устойчивости функционирования КИИ в условиях ИПВ соответствует значениям параметров сенсоров ИПВ, которые находятся в зоне своих допустимых значений. Допустимое значение риска нарушения устойчивости функционирования КИИ по принципу ALARP (верхняя часть области ALARP) обеспечивается только при нахождении параметров сенсоров ИПВ в установленных интервалах значений.

Оценку риска нарушения устойчивости функционирования КИИ в условиях ИПВ предлагается осуществить с использованием сенсоров ИПВ путем сигнатурного и эвристического контроля эмоциональной окраски и тональности (например, экстремистской) текстовой, графической, картографической и звуковой информации в социальных сетях, электронных средствах массовой информации, мобильных приложениях и других приложениях сети Интернет.

В соответствии с таблицей 1, частоте возникновения отказов КИИ (10^{-9} 1/ч) и риску, не принимаемому в расчет, будет соответствовать допустимое значение вероятности безотказной работы КИИ в условиях ИПВ $R_{НАП} \geq 0,9$ и минимальное значение ущерба срыва ТЦУ ПТЭ в результате невыполнения необходимых действий операторами КИИ.

Таблица 1

Оценка допустимого риска нарушения устойчивости функционирования КИИ в результате успешных ИПВ

Уровень риска	Частота возникновения отказов	Оценка уровня устойчивости функционирования КИИ	Значения ущерба за счет отказа КИИ (баллы)
Недопустимый	10^{-3} 1/ч	$0,5 \leq P_{\text{НАП}} \leq 0,6$	$\gamma_{\text{в}} = 6 \div 10$
Нежелательный	10^{-5} 1/ч	$0,6 \leq P_{\text{НАП}} \leq 0,7$	$\gamma_{\text{с}} = 4 \div 5$
Допустимый	10^{-8} 1/ч	$0,7 \leq P_{\text{НАП}} \leq 0,9$	$\gamma_{\text{с}} = 2 \div 3$
Не принимаемый в расчет	10^{-9} 1/ч	$P_{\text{НАП}} \geq 0,9$	$\gamma_{\text{н}} = 1$

Значения допустимого риска нарушения устойчивости функционирования КИИ получим с использованием математического выражения [25]:

$$R_{\text{доп}} = \sum_{i=1}^n ((1 - P_{\text{ИПВ}i}) \gamma_j), \quad (11)$$

где: $P_{\text{ИПВ}i}$ – вероятность безотказной работы КИИ с i -м сенсором обнаружения ИПВ, γ_j – значение ущерба j -го уровня от ИПВ (определяется экспертным путем).

Для оценивания риска в соответствии с принципом ALARP возможно использовать четыре установленные категории рисков. Оценка риска заключается в сопоставлении риска, рассчитанного на основе фактических данных, с установленной шкалой риска и присвоении риску по результатам сравнения одной из четырех категорий (табл. 1). Каждой из категорий рисков, соответствует определенный диапазон значений уровня риска, в соответствии со шкалой риска, принятой для риска данного вида.

Потенциально возможный ущерб КИИ в условиях ИПВ определяется задачами, выполняемыми как КИИ в целом, так и отдельными ПТЭ, а также режимами функционирования (например, режимом реального масштаба времени). Причем необходимо рассматривать ущерб, обусловленный невыполнением функциональных задач операторами КИИ, так и от ложных (дестабилизирующих) сообщений о функциональных нарушениях в КИИ, требующих оперативного вмешательства с затратой определенных ресурсов.

Заключение

Таким образом, в статье предложена методика, которая позволяет на основе классификации комплексных информационно-технических и информационно-психологических воздействий и экспериментальных исследований определить значение вероятностно-временных показателей обеспечения устойчивости критической информационной инфраструктуры для установления наиболее опасных угроз и уязвимостей, и установки сенсоров информационных воздействий.

Литература

1. Климов С.М., Астрахов А.В., Сычев М.П. Методические основы противодействия компьютерным атакам. Электронное учебное издание. – М.: МГТУ имени Н.Э. Баумана, 2013. 110 с.
2. Гапич А.Э., Лушников Д.А. Технологии цветных революций: Монография. – 2-е изд. – М.: РИОР: ИНФРА-М, 2016. 126 с.
3. Овчинский В.С. Новая стратегия кибербезопасности США. Международный научно-аналитический журнал «Стратегические приоритеты», выпуск 4 (8), 2015. С. 15 – 32.
4. Кларк, Р., Нейк, Р. Третья мировая война: какой она будет? – СПб.: Питер, 2011. 336 с.
5. 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.
6. Угрозы информационной безопасности в кризисах и конфликтах XXI века / Под ред. А.В. Загорского, Н.П. Ромашкиной – М.:ИМЭМО РАН, 2015. 151 с.
7. Операции информационно-психологической войны: краткий энциклопедический словарь-справочник / В.Б. Вепринцев, А.В. Манойло, А.И. Петренко, Д.Б. Фролов; под ред. А.И. Петренко – 2-е изд., стереотип. – М.: Горячая линия – Телеком, 2017. 495 с., ил.
8. Основы инфокоммуникационных технологий. Учебное пособие для вузов / В.В. Величко, Г.П. Катунин, В.П. Шувалов; под ред. Профессора В.П. Шувалова. – М.: Горячая линия-Телеком, 2009. 712 с., ил.
9. Володенков С.В. Интернет-коммуникации в глобальном пространстве современного политического управления. – М.: Издательство Московского университета; Проспект, 2018. 272 с., ил.

10. Критически важные объекты и кибертерроризм. Часть 1. Системный подход к организации противодействия / О.О. Андреев и др. Под ред. В.А. Васенина. – М.: МЦНМО, 2008. 398 с.
11. Климов С.М., Сосновский Ю.В. Методика оценки защищенности микропроцессорных систем управления в условиях информационно-технических воздействий // Надежность. 2018. Том 18. №4. С. 36-44.
12. Роговский Е.А. Выборы в США: Триумф цифровой демократии? Научный и общественно-политический журнал Института США и Канады Российской академии наук. №4. 2017. С 5-14.
13. Шубинский И.Б. Структурная надежность информационных систем. Методы анализа/ И.Б. Шубинский – Ульяновск: Областная типография «Печатный двор», 2012. 216 с., ил.
14. 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.
15. 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.
16. Астрахов А.В., Правиков Д.И., Сычев М.П., Тягунков О.И. Применение методов кластеризации для анализа неиндексируемых Интернет-ресурсов // Инженерный журнал: наука и инновации, №2(14), 2013. <http://engjournal.ru/articles/531/531.pdf>.
17. Климов С.М., Купин С.В., Купин Д.С. Модели вредоносных программ и отказоустойчивости информационно-телекоммуникационных сетей // Надежность. 2017. № 4. С. 36-43. DOI: 10.21683/1729-2640-2017-17-4.
18. Астрахов А.В., Куликов Л.С., Минаев В.А. Моделирование угроз информационных воздействий манипулятивного характера // Вопросы радиоэлектроники. 2016. № 12. С. 63-69.
19. Шубинский И.Б. Надежные отказоустойчивые информационные системы. Методы синтеза / И.Б. Шубинский – Ульяновск: Областная типография «Печатный двор», 2016. 544 с., ил.
20. Гапанович В.А., Розенберг Е.Н., Шубинский И.Б. Некоторые положения отказобезопасности и киберзащищенности систем управления // Надежность. 2014. №2. С. 88-100.
21. Гнеденко Б.В. Курс теории вероятностей: Учебник / Предисл. А.Н. Ширяева. Изд. 11-е – М.: ЛЕНАНД. 2015. 448 с.
22. К. Капур, Л. Ламберсон. Надежность и проектирование систем. Под ред. И.А. Ушакова. Пер. с англ. – М.: «Мир», 1980. 604 с., ил.
23. Гапанович В.А., Шубинский И.Б., Замышляев А.М. Метод оценки рисков системы из разнотипных элементов // Надежность. 2016. Том 16. № 2. С. 49-53.
24. Климов С.М., Котляшев Н.Н. Метод регулирования рисков комплексов средств автоматизации в условиях компьютерных атак // Надежность. 2013. №2. С. 93-107.
25. Шубинский И.Б. Функциональная надежность информационных систем. Методы анализа / И.Б. Шубинский. – Ульяновск: Областная типография «Печатный двор», 2012. 296 с., ил.

PROCEDURE FOR ASSURING THE CONTINUITY OF CRITICAL INFORMATION INFRASTRUCTURE UNDER CONDITIONS OF INFORMATION INFLUENCE

Klimov S.M.⁶, Polikarpov S.V.⁷, Rizhov B.S.⁸, Tihonov R.I.⁹, Shpirnya I.V.¹⁰

The purpose of the article is to develop a procedure that would allow defining the probabilistic and temporal indicators ensuring continuity of the critical information infrastructure in conditions of information influence. The information influence includes a complex of information, technical and information and psychological influences. As applied to the critical information infrastructure, vulnerabilities of information and telecommunication systems and vulnerabilities of automated process control systems to information and technical influence and vulnerability of the human operator to information and psychological influence are considered. The elements of critical information infrastructure are interrelated human-machine systems where the information influence exerted on the operator and/or computer equipment leads to degraded performance of the critical information infrastructure on the whole.

Information and technical influence is considered to be purposeful software actions produced on the software and information of the critical information infrastructure in order to temporarily disrupt its operation processes.

-
- 6 Sergey Klimov, Dr.Sc., Professor, Central Research Institute of the Russian Defense Ministry, Korolev, Russia. E-mail: klimov.serg2012@yandex.ru
 - 7 Sergey Polikarpov, Central Research Institute of the Russian Defense Ministry, Korolev, Russia. E-mail: polikarpov.s.v@yandex.ru
 - 8 Boris Rizhov, Ph.D., Associate Professor, Central Research Institute of the Russian Defense Ministry, Korolev, Russia. E-mail: ryzhov5@yandex.ru
 - 9 Rudolf Tihonov, Central Research Institute of the Russian Defense Ministry, Korolev, Russia. E-mail: tihonovrudolf@mail.ru
 - 10 Igor Shpirnya, General Staff of the Armed Forces of the Russian Federation, Moscow, Russia. E-mail: z@mil.ru

Information and psychological influence is the influence produced on operators and residents in the places of the critical information infrastructure placement through social media, electronic media, mobile applications, and other internet resources leading to *destabilization, disruption of operating modes, and reduced reliability of the critical information infrastructure operation. Realization of the threat of combined information, technical and psychological influence is possible in case vulnerabilities exist in the critical information infrastructure and internet resources are available for operators and residents in the areas of the critical information infrastructure operation.*

The procedure is based on the following assumptions: probabilistic and temporal indicators of the critical information infrastructure are evaluated based on the findings of experimental studies performed on the cyber range; simulators of information influence exist; continuity is assured using structural and functional redundancy; standard sensors have been developed to detect, prevent, and liquidate the consequences of information influence; response to computer incidents is provided in the form of the system operability restoration.

Within the scope of the procedure, probabilistic and temporal indicators have been developed to ensure the continuity of critical information infrastructure under information and technical influence and to assess the risks of information and psychological influence produced on operators and residents in the places of infrastructure elements location.

Keywords: probabilistic-temporal indicators, information and technical impacts, information and psychological impacts, information impact sensors, vulnerabilities, risks of impaired functioning, information security tools.

References

1. Klimov S.M., Astrahov A.V., Sichev M.P. Metodicheskie osnovi protivodeistviy kompiutornum atakam. Elektronnoe uchebnoe izdanie. – M.: MGITU imeni N.E. Bauman, 2013. 110 s.
2. Gapich A.E., Luchnikov D.A. Tekhnologii cvetnukh revolucii: Monografii. – 2 – e izd. – M.: RIOR: INFRA-M, 2016. 126 s.
3. Ovchinskii B.S. Novaj strategij kiberbezopasnosti SUA. Megdunarodnui nauchno-analiticheskii zhurnal «Strategicheskie prioritety», vypusk 4 (8), 2015. S. 15-32.
4. Klark, R., Neik, R., Tretij mirovaj voina: kakoi ona budet? – SPb.:Piter, 2011.336 s.
5. Antonov S.G., Klimov S.M., Metodika ozenki riskov naruchenij ustoichivosti funkcionirovanij programno-apparatnukh kompleksov v usloviykh informacionno-tehnicheskikh vozdeistvii //Nadezhnost. 2017. Tom 17.№1.S32-39.
6. Ugrosi informacionnoi bezopasnosti v krizisakh i konfliktakh XXI veka / Pod red. A.V. Zagorskogo, N.P.Romachkinoi – M.: IMEMO RAN, 2015. 151 s.
7. Operazii informacionno-psikhologicheskoi vojni: kratkii ensiklopedicheskii slovar-spravochnik/ V.B.Vepinzev, A.V. Manoilo, A.I. Petrenko, D.B. Frolov; pod red. A.I. Petrenko – 2-e izd., stereotip. – M.: Gorjchaj linij – Telekom, 2017. 495 s., il.
8. Osnovi infokommunikacionnukh tehnologij. Uchebnoe posobie dlj vyzov/ V.V. Velichko, G.P. Katunin, V.P.Chuvalov; pod red. Professora V.P. Chuvalova. – M.: Gorjchaj linij – Telekom, 2009. 712 s., il.
9. Volodenkov S.V. Internet-kommunikazii v globalnom prostranstve sovremennogo politicheskogo upravlenij. – M.: Izdatelstvo Moskovskogo universiteta; Prospekt, 2018.272s., il.
10. Kriticheski vazhnie obekti i kiberterrorizm. Chast 1. Sistemui podchod k organizacii protivodeistviy./ O.O.Andreev i dr. Pod red. V.A.Vasenina.- M.:MCNMO, 2008. 398 s.
11. Klimov S.M., Sosnovskii J.V. Metodika ozenki zachichennosti mikroprocessornich system upravlenij v usloviykh informacionno-technicheskikh vozdeistvii//Nadezhnost. 2018. Tom 18. №4. S.36-44.
12. Rogovskii E.A. Vuboru v USA: Triumf cifrovoi demokratii? Nauchnui i obchestvenno-politicheskii zhurnal Instituta USA i Kanadu Rossiiskoi akademii nauk.№4. 2017. S 5 -14.
13. Chubinskii I.B. Strukturnaj nadezhnost informacionnikh system. Metodi analiza/ I.B. Chubinskii. – Uliynovsk: Oblastnaj tipografij «Pechatnij dvor», 2012. 216 s., il.
14. Klimov S.M., Polovnikov A.Y. Sergeev A.P. Model funkcionainoi otkazoustoichivosti processov obespechenij potrebitelei navigacionnumi signalami v slozhnukh usloviykh// Nadezhnost. 2017. Tom 17. №2. S. 41-47.
15. Klimov S.M., Polikarpov S.V., Fedchenko A.V. Metodika povuchenij otkazoustoichivosti setei sputnikovoi svijzi v usloviykh infomacionno-tehnicheskikh vozdeistvii.// Nadezhnost. 2017. Tom 17. №3. S. 32-40.
16. Astrahov A.V., Pravikov D.I., Suhev M.P., Tjgunkov O.I. Primenenie metodov klasterizacii dlj analiza neindeksiruemich Internet-resursov\ Inzhenernui zhurnal: nauka i innovazii, № 2(14), 2013. <http://engjournal.ru/articles/531/531.pdf>.
17. Klimov S.M., Kupin S.V., Kupin D.S. Modeli vredonosnukh program i otkazoustoicivosti informacionno-telekommunikacionnukh setei// Nadezhnost. 2017. №4 S.36-43. DOI: 10.21683/1729-2640-2017-17-4.
18. Astrahov A.V., Kulikov L.S., Minaev V.A. Modelirovanie ugroz informacionnukh vozdeistvii manipuljativnogo charaktera. Avoprosu radioelektroniki. 2016. №12. S.63-69.
19. Chubinskii I.B. Nadezhnie otkazoustoichivue informacionnue sistemu. Metodu sinteza/ I.B. Chubinskii.- Uliynovsk: Oblastnaj tipografij «Pechatni dvor», 2016. 544 s., il. – («Zhurnal nadezhnost»).
20. Gapanovich V.A., Rozenberg E.N., Chubinskii I.B. Nekotorue polozenij otkazobezopasnosti i kiberezachichennosti system upravlenij// Nadezhnost. 2014. №2. S.88-100.
21. Gnedenko B.V. Kurs teorii verojtnostei: Uchebnik/Predisl. A.N. Chirjeva. Izd. 11-e – M.:LENAND. 2015. 448 s.
22. K.Kapur., L.Lamberson. Nadezhnost i proektirovanie sistem. Pod ped. I.A. Uchakova. Per. S angl. – M.: «Mir», 1980. 604 s., il.

23. Gapanovich V.A., Chubinskii I.B., Zamuchljev A.M. Metod ozenki riskov sistemu iz raznotipnuch elementov// Nadezhnost. 2016. Tom 16. №2 s.49-53.
24. Klimov S.M., Kotjchev N.N. Metod regulirovanij riskov kompleksov sredstv avtomatizacii v uslovijch kompjyternuch atak// Nadezhnost. 2013. №2 s. 93-107.
25. Chubinskii I.B., Funkcionalnaj nadezhnost informacionnuch system. Metodu analiza/ I.B Chubinskii. - Uljnovsk: Oblastnaj tipografij «Pечатnui dvor», 2012. 296 s., il.