ПОВЫШЕНИЕ УСТОЙЧИВОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ К ЦЕЛЕВЫМ КОМПЬЮТЕРНЫМ АТАКАМ

Лапсарь А.П.[1], Назарян С.А.[2], Владимирова А.И.[3]

Цель статьи: *повышение безопасности значимых объектов критической информационной инфраструктуры в условиях деструктивного информационного воздействия, реализуемого в форме целевых атак.*

Методы: *компаративный анализ в рамках системного подхода; марковская теория эволюционных процессов; синергетика.*

Полученный результат: *выполнен анализ свойств целевых атак и особенностей их воздействия на критическую информационную инфраструктуру. Для выявления целевых атак обосновано применение сочетания различных методов обнаружения с приоритетом эвристического анализа. Разработана схема реализации метода оценки состояния объекта критической информационной инфраструктуры на базе модифицированной марковско-параметрической модели с интегрированной в ее структуру системой выявления компьютерных атак. Предложено предварительную оценку опасности компьютерных атак и выработку рекомендаций по их нейтрализации проводить параллельно с оценкой свойств и характеристик деструктивного информационного воздействия.*

Научная значимость: *расширена область применения марковско-параметрических моделей за счет адаптации к нештатным условиям; синтезирован алгоритм обнаружения целевых компьютерных атак путем комплексирования различных методов анализа.*

Ключевые слова: *деструктивное информационное воздействие, целевая атака, марковская параметризованная модель, оценка состояния, объект критической информационной инфраструктуры.*

DOI:10.21681/2311-3456-2022-2-39-51

Введение

Широкое использование информационных технологий породило проблему защиты от противоправных действий в виртуальном пространстве [1-3]. Количество киберинцидентов во всем мире вырастает ежегодно в полтора-два раза, в том числе – компьютерных атак на системы управления процессами производства и обеспечения жизнедеятельности. Значительная доля преступлений – целевые атаки на объекты критической информационной инфраструктуры (далее – объекты КИИ), реализующие управление важнейшими элементами инфраструктурного обеспечения (далее – ВЭИО) [2,4]. Целевая атака как адресное, скрытное, четко спланированное, продолжительное, использующее различные инструменты и методы, управляемое воздействие является одним из ключевых элементов современных киберпреступлений[4]. Важность задачи защиты инфраструктуры от киберпреступников вывела проблему повышения устойчивости объектов КИИ к деструктивным информационным воздействиям на государственный уровень [5-8].

В настоящее время для обеспечения безопасности объектов КИИ государственное регулирование предусматривает применение сил и средств защиты от деструктивного воздействия. Состав средств обеспечения безопасности объектов КИИ нормативно

[4] Отчет Positive Technologies [Электронный ресурс] – Режим доступа https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q2/

[1] Лапсарь Алексей Петрович, кандидат технических наук, доцент, заместитель начальника отдела Управления ФСТЭК России по Южному и Северо-Кавказскому федеральным округам, г. Ростов-на-Дону, Россия. E-mail: lapsarap1958@mail.ru

[2] Назарян Сергей Ашотович, доцент кафедры «Информационных технологий и защиты информации» ФГБОУ ВО «Ростовский государственный экономический университет (РИНХ)», г. Ростов-на-Дону, Россия. E-mail: serj_nazaryan@mail.ru

[3] Владимирова Алиса Игоревна, магистрант ФГБОУ ВО «Ростовский экономический университет (РИНХ)», Ростов-на-Дону, Россия. E-mail: alisa.v@mail.ru

определяется исходя из их категории значимости. При этом при определении необходимого состава и характеристик средств защиты от деструктивного воздействия не учитываются особенности конкретной КИИ, условия ее функционирования, взаимодействие с управляемой системой и другие важные аспекты.

Исследование проблемы повышения устойчивости объектов КИИ к деструктивным информационным воздействиям и обеспечения их безопасности осуществляется, как правило, только с точки зрения способности противостоять компьютерным атакам без учета надежности, взаимодействия с внешней средой и смежными системами, условий функционирования и других факторов [9-11]. Предлагаемые ранее математические модели КИИ не учитывают всех аспектов их функционирования, а также не рассматривают проблемы, связанные с обеспечением управления ВЭИО при деструктивном воздействии.

В работах [10,12] предложена модель функционирования КИИ в условиях, связанных с реализацией деструктивного информационного воздействия. Вместе с тем, рассмотренные модели предполагают наличие априорной информации о свойствах и характеристиках компьютерной атаки. В случае же осуществления целевой компьютерной атаки возникают трудности не только с определением ее свойств и характеристик, но и с ее обнаружением.

Настоящая работа посвящена повышению устойчивости КИИ к деструктивным информационным воздействиям путем адаптации марковско-параметрической модели защищаемого объекта к условиям неопределенности, связанным с обнаружением целевых атак.

1. Функционирование КИИ в условиях актуальной угрозы деструктивного информационного воздействия

Так как, исходя из условий эксплуатации, КИИ является открытой системой, осуществляющей взаимодействие с сопряженными информационными системами, то не исключена реализация удаленного деструктивного информационного воздействия со стороны злоумышленников. При этом продолжительность подготовки и реализации деструктивного информационного воздействия на КИИ может осуществляться в течение длительного времени [2,6,13].

Потеря работоспособности КИИ не проявляется мгновенно в виде скачкообразного процесса, а является следствием снижения качества основных показателей ее функционирования и их выхода за границы допусков. Процесс изменения показателей, характеризующих качество функционирования, занимает некоторый промежуток времени, определяемый исходными значениями показателей, а также различными влияющими факторами [10,12,14-16].

Таким образом, встает задача поддержания КИИ в работоспособном состоянии в течение некоторого времени, необходимого для проведения мероприятий по нейтрализации негативных последствий воздействия. Отказ КИИ следует определять как событие, заключающееся в выходе характеристик ее функционирования за установленные пределы, то есть происходит накопление неисправности, отказ «развивается» во времени [9,14]. Состав и объем мероприятий по повышению устойчивости КИИ к деструктивным воздействиям и нейтрализации угроз информационной безопасности базируется не только на оценке текущего состояния КИИ, но и на прогнозе их изменения на некоторый отрезок времени, необходимый для принятия соответствующих мер. При этом проблему обеспечения безопасности функционирования КИИ в условиях деструктивного информационного воздействия следует рассматривать в комплексе с обеспечением ее технической надежности и безопасности [12,16].

Условиями оптимального управления являются правильная оценка исходного состояния объекта и адекватность управляющих воздействий, то есть нахождение КИИ в исправном состоянии [16-19]. С целью обеспечения названных условий обоснуем объем функций безопасности, реализуемых объектом КИИ при деструктивном воздействии.

В нормальных условиях эксплуатации КИИ обеспечивает реализацию некоторого набора полезных функций управления $N(x,\omega,t)$, который определяет качество и показатели эффективности (в том числе экономические) функционирования ВЭИО в отсутствии деструктивного информационного воздействия $\omega = 0$. При этом КИИ реализует некоторый набор функций безопасности $B(x,\omega,t)$, требующий определенного объема расходования его ресурсов. Одним из показателей качества и эффективности функционирования объектов КИИ считается доля его ресурса, используемого на реализацию функций по предназначению $R|_{N(x,\omega,t)} - R|_{B(x,\omega,t)} = R|_{M(x,\omega,t)} \to \max$. В нормальных условиях при $\omega = 0$ это условие обеспечивается соотношением $B(x,\omega,t) = \min$, которое осуществляется средствами, выполняющими минимально необходимый набор функций безопасности, например, – только защиту от несанкционированного доступа, мониторинг или выборочный контроль [10].

В условиях деструктивного воздействия набор функций безопасности существенно расширяется за счет необходимости купирования возникающих угроз, следовательно, возрастает доля ресурса объектов КИИ, расходуемого на реализацию функций безопасности $R|_{B(x,\omega,t)}$ и уменьшается доля «полезного» ресурса $R|_{M(x,\omega,t)}$. При достижении некоторой минимально допустимой величины $R|_{M(x,\omega,t)} \geq R_{\text{доп}}|_{M(x,\omega,t)}$ продолжение эксплуатации объектов КИИ становится нецелесообразным, требуется прекратить его эксплуатацию и произвести аварийную остановку ВЭИО.

Поскольку КИИ является сложным объектом, деструктивное воздействие не приводит к нарушению работоспособности, а только ухудшает характеристики его функционирования. В этом случае значение $R_{\text{доп}}|_{M(x,\omega,t)}$ может быть рассчитано на основе классического показателя «эффективность-стоимость» или получено методами экспертной оценки. Так как КИИ является техническим объектом, в качестве основы для определения $R_{\text{доп}}|_{M(x,\omega,t)}$ можно использовать вероятность сохранения ее работоспособности в условиях деструктивного воздействия $P(x,\omega,t)$ в течение времени до наступления необратимых изменений в КИИ $T(x,\omega)$, приводящих к аварии ВЭОИ. При этом должны учитываться параметры деструктивного воздействия, уровень которых не должен превышать априори заданного допустимого значения $R_{\text{доп}}|_{M(x,\omega,t)} = F\left[P(x,\omega,t), T(x,\omega)\right] \ \forall \ \omega(t) < \omega_{зад}(t)$. Для оценки названных выше характеристик функционирования КИИ воспользуемся эволюционной моделью, обоснование которой применительно к КИИ приведено в [12]. Рассмотрим функционирование КИИ в различных условиях с использованием названной модели, для чего разделим процесс его функционирования на два этапа: этап нормальной эксплуатации и этап нештатной эксплуатации, обусловленной деструктивным информационным воздействием.

Использование предложенной в работах [10,12] марковско-параметрическая модели КИИ позволяет оперативно реагировать на возможные деструктивные информационные воздействия на КИИ с целью принятия мер по купированию последствий таких воздействий и повышению эффективности и безопасности эксплуатации ВЭОИ, функционирующего под управлением КИИ. Математическая модель КИИ представляет собой описание эволюции диффузионного процесса изменения ее состояния во времени в виде параметризованного дифференциального уравнения в частных производных

$$\frac{\partial\lambda(x,\omega,t)}{\partial t} = -a(x,\omega,t)\frac{\partial\lambda(x,\omega,t)}{\partial x} + \frac{1}{2}b(x,\omega,t)\frac{\partial^2\lambda(x,\omega,t)}{\partial x^2}. \quad (1)$$

Здесь $\lambda(x,\omega,t)$ характеризует переходную плотность вероятности распределения диффузионного процесса $x(\omega,t)$, а $a(x,\omega,t)$ и $b(x,\omega,t)$ — его локальные характеристики (коэффициенты сноса и диффузии). Поскольку плотность вероятности распределения стохастического процесса является наиболее информативной характеристикой, получив решение (1) несложно вычислить основные стохастические характеристики КИИ, на базе которых будет принято решение о ее дальнейшей эксплуатации.

Приближенное решение исходного уравнения (1) с использованием метода Галеркина предлагается синтезировать на основе степенных полиномов $\lambda_n(x,\omega,t) = \sum_{i=1}^{n}\sum_{k=1}^{N} v_{ik}\omega^k\gamma_i(x,t)$ или полиномов Лагранжа $\lambda_n(x,\omega,t) = \sum_{i=1}^{n}\sum_{k=1}^{N} c_{ni}\left(\omega_{(k)}\right)L_k(\omega)\gamma_i(x,t)$ [4,10]. Оценка (вычисление) основных стохастических характеристик функционирования КИИ на основе полученных базовых решений уравнения (1) производится сразу в аналитическом виде, что позволяет существенно повысить оперативность оценки состояния КИИ и скорость реагирования на компьютерные атаки.

Для оценки возможности продолжения эксплуатации КИИ в условиях деструктивного воздействия предлагается вычислить его параметрическую надежность на некоторый интервал времени и время нахождения основных параметров функционирования в пределах допустимой области [9,12]. Надежность, на основе базовых решений вычисляется по формуле $F(x,\omega,t) = \int_{g_{\min}}^{x}\lambda(x,\omega,t)dx$, а время достижения процессом $x(\omega,t)$ границ допустимой области – $T_n(\omega) = \int_0^{\infty} t^n f(x,\omega,t)dt, \ \ n=1.$

Названные выше стохастические характеристики являются функциями не только от времени, но и от параметра ω, который характеризует свойства деструктивного воздействия. При условии нахождения параметра ω в пределах области Ω состояние работоспособности КИИ ограничивается минимальным значением вероятности для оптимистической оценки и максимальным — для гарантированной оценки.

Структурная схема объекта КИИ, реализующая описанную выше марковско-параметрическую модель, представлена на рис. 1.

Представим процесс функционирования КИИ в виде трех периодов.

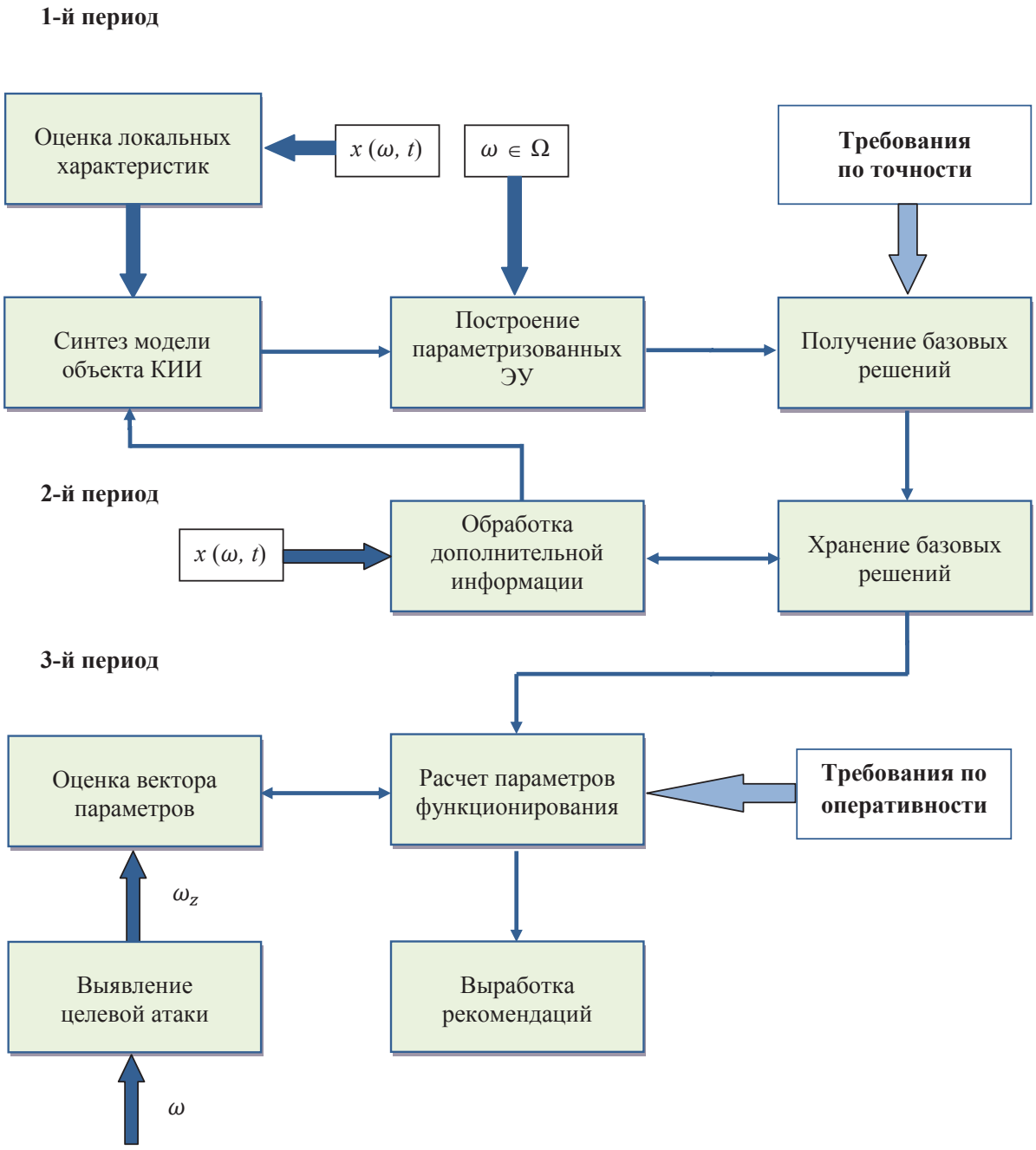

Рис. 1. Структурная схема объекта КИИ на базе марковско-параметрической модели

Первый, или начальный период характеризуется подготовкой к штатному функционированию КИИ. Его основное содержание состоит в формировании возможной области свойств и характеристик параметра, получении локальных характеристик исследуемого процесса в параметрическом виде, синтезе модели объекта КИИ, вычислении опорных решений, выборе возможных вариантов управления, Для этого используются все доступные источники: статистическая информация о техническом состоянии КИИ, банки данных угроз, известные на текущий момент деструктивные воздействия, алгоритмы действий злоумышленников и другие.

Второй период представляет собой штатную эксплуатацию КИИ, здесь осуществляется уточнение модели объекта с использованием поступающей дополнительной информации, а также выявление признаков возможного деструктивного информационного воздействия.

Переход функционирования КИИ в третий период происходит при наличии деструктивного информационного воздействия. Ключевым моментом третьего

периода является своевременное обнаружение деструктивного информационного воздействия и оценка его характеристик. Конкретное значение параметра ω используется для подстановки в заранее синтезированные базовые решения уравнения (1). Выводы по дальнейшей эксплуатации КИИ и управляемых ею ВЭИО принимается в соответствии с алгоритмом, представленным в [10].

Функционирование объектов КИИ в описанных выше периодах возможно только при условии достаточности информации о свойствах и характеристиках деструктивного информационного воздействия (компьютерной атаки). Технические системы и управляющие ими КИИ являются уникальными, следовательно, компьютерные атаки на них имеют специфические особенности, связанные с конкретным объектом атаки. Поскольку целевая атака готовится для воздействия на конкретную КИИ и может использовать специфические разработки, используемая модель нуждается в доработке, исходя из складывающейся обстановки путем адаптации к «незнакомым» условиям. Основной проблемой функционирования объектов КИИ при целевой компьютерной атаке является расширение области определения параметра, в результате чего значения параметра уходят за границы допустимой области и становятся неопределенными. Применение в этих условиях марковско-параметрической модели предполагает оценку масштаба расширения области определения параметра и ее новые границы, для чего необходимо исследовать основные особенности целевых атак на КИИ.

2. Основные свойства целевых атак

Описание свойств целевых атак проведем с точки зрения опасности для КИИ, управляющего сложными системами, функционирующими в наиболее значимых сферах[5]. Как отмечалось выше, целевые атаки — это атаки, нацеленные на конкретную КИИ [6], важнейшей их особенностью является сложность выявления, так как они уникальны, спланированы под конкретную информационную систему.

Целевые атаки направлены на достижение конкретной цели и состоят из нескольких стадий. Инициаторы целевых атак детально изучают особенности КИИ, выявляют слабые места, находят уязвимости, выясняют особенности средств защиты и построения самой КИИ для создания адаптированного под атакуемую КИИ вредоносного программного обеспечения, способного обойти системы защиты. Данные атаки могут продолжаться длительный период времени и не всегда своевременно обнаруживаются [4, 5,7,20].

Таким образом, главными признаками и особенностями целевых атак с точки зрения опасности для КИИ являются следующие: атаки направлены на конкретные КИИ; реализуются длительный период времени; не использовались ранее на других объектах; вредоносное программное обеспечение разрабатывается под конкретную атаку; могут применяться уязвимости нулевого дня[6].

Целевая атака всегда следует четко спланированной стратегии, которая чаще всего состоит из четырех основных фаз [2-4,8,20].

Фаза подготовки состоит в определении цели, с учетом которой происходит сбор информации для выявления уязвимых мест в защите КИИ. По результатам этой работы разрабатывается стратегия незаконного проникновения (взлома), а также формируется набор инструментов для преодоления механизмов защиты. На последнем этапе фазы проводятся эксперименты для повышения эффективности атаки и наиболее полного достижения результата.

Фаза проникновения заключается во внедрении вредоносного программного обеспечения в КИИ, при этом применяются комбинированные техники для преодоления средств защиты. В рамках конкретной фазы могут использоваться методы социальной инженерии.

Фаза закрепления предполагает распространение вредоносного программного обеспечения внутри КИИ.

Финальная фаза целевой атаки – это реализация механизмов достижения поставленной цели, которая может заключаться в нарушении функционирования, снижении показателей качества, искажении ключевой информации, организации «люков» для последующих атак и так далее. В ряде случаев финальная стадия предполагает маскировку следов проникновения в КИИ.

При целевых атаках, как правило, применяются те же приемы, что и при обычных. Основное отличие заключается в воздействии на особые компоненты КИИ, а также применении навыков социальной инженерии для выявления характеристик КИИ и особенностей ее защиты.

Технологии успешных целевых атак распространяются на другие аналогичные объекты[7] [2,4,21].

5 Указаны в Федеральном законе от 26 июля 2017 года N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

6 Передовая защита от сложных угроз и снижение риска целевых атак [Электронный ресурс] – Режим доступа https://media.kaspersky.com/ru/businesssecurity/Kaspersky_Anti_Targeted_Attack_ Platform_Whitepaper_RU.pdf

7 Безопасность объектов КИИ [Электронный ресурс] – Режим доступа https://www.ptsecurity.com/ru-ru/solutions/bezopasnost-kii/

В настоящее время набольшее распространение получили сетевые и системные целевые атаки. Сетевые атаки предполагают захват управления или повышение привилегий для контроля над КИИ. К основным видам сетевых атак принадлежат[8] IP-спуфинг, парольные атаки, SQL-инъекции, уязвимости нулевого дня. Системные атаки используют уязвимости в системных программах, основные из них это DoS- и DDoS- атаки, черви, вирусы [1,4,7,13]. Результатами деструктивного информационного воздействия могут быть полный или частичный отказ КИИ, нарушение штатного режима функционирования, ухудшение ее качества, снижение эффективности системы безопасности и другие. Кроме прямых потерь от нарушения штатного режима функционирования КИИ следует учитывать и косвенные. К ним относятся репутационные потери, судебные издержки, расход ресурсов на отражение деструктивного воздействия и ликвидацию его последствий: расход времени, материальных средств, человеческих ресурсов, блокировка участков памяти и других.

Своевременное и эффективное противодействие целевым атакам на КИИ возможно только при условии их своевременного обнаружения.

3. Методы обнаружения и защиты от целевых атак

Основным источником сведений для обнаружения целевых атак является анализ процесса функционирования КИИ[9], а именно сетевого трафика, событий безопасности, потребляемых ресурсов, целостности объектов файловой системы [4,13,21].

Некоторая часть ресурсов системы (КИИ) $R\big|_{B(x,\omega,t)}$ выделяется для записи и анализа трафика, что позволяет накапливать статистическую информацию для формирования эталонной модели поведения КИИ. Это позволяет контролировать динамику изменения трафика и путем его мониторинга выявлять признаки атак. Анализ сетевого трафика позволяет обнаруживать отправку неопределенных пакетов, наличие в сети компьютеров или программ, которые не должны там присутствовать и так далее[10]. События безопасности фиксируются в журналах событий, куда записываются значимые события, в частности ошибки и сбои в работе КИИ, попытки некорректных и неправильных вводов данных при входе в систему, а также все операции, совершаемые под учетной записью.

Основными ресурсами, потребляемыми в процессе функционирования КИИ, являются процессорное время, память, каналы ввода-вывода, периферийные устройства. Их мониторинг позволяет идентифицировать угрозу в общем виде. Контроль целостности объектов файловой системы позволяет определить изменения в используемых программах. Вычисление контрольных сумм для всех важных бинарных и конфигурационных файлов в системе и сравнение их с предыдущими записями, хранящимися в базе данных, может предупредить о наличии несоответствий или модификациях. Организаторы целевых атак изменяют файлы или объекты с целью размещения вредоносных программ или создания «back door», которые позволяют незаметно совершать вход в систему или подключаться к другим компьютерам, а также для маскировки деструктивного воздействия.

Важнейшим способом обнаружения целевых атак является отслеживание всех возможных аномалий в поведении КИИ, в запрашиваемых командах, в запускаемых кодах. Выявленные аномалии приравниваются к атаке, что в дальнейшем позволяет применить алгоритмы защиты. Это обеспечивает выявление атак на ранних этапах их появления с последующей их нейтрализацией. Однако, приравнять аномалию к атаке можно с какой-то вероятностью, поэтому обнаружение аномалий сопровождается последующим углубленным исследованием для однозначной идентификации атаки. Поскольку КИИ функционирует совместно с ВЭИО, при анализе аномалий необходимо в обязательном порядке учитывать показания средств измерений КИИ, то есть измерительной составляющей системы контроля и управления.

В настоящее время известны следующие основные методы выявления целевых атак: сигнатурный анализ, анализ аномальной сетевой активности (аномальных операций), поведенческий анализ рабочих станций, эвристический анализ.

В системах обнаружения компьютерных атак наибольшее распространение получил сигнатурный анализ. Он основан на обнаружении уже известных угроз путем анализа журнала регистрации событий или сетевого трафика. Сигнатурный анализ позволяет обнаружить атаку на начальной стадии и предотвратить ее дальнейшую реализацию, его удобно использовать в рамках марковско-параметрических моделей [4,6,10].

8 Сетевые атаки. Виды. Способы борьбы [Электронный ресурс] – Режим доступа https://moluch.ru/conf/tech/archive/5/1115/

9 Актуальные вопросы выявления сетевых атак [Электронный ресурс] – Режим доступа http://www.infosecurity.ru/_gazeta/content/030211/article07.html

10 Проблемы обработки статистики сетевого трафика для обнаружения вторжений в существующих информационных системах [Электронный ресурс] – Режим доступа https://cyberleninka.ru/article/n/problemy-obrabotki-statistiki-setevogo-trafika-dlya-obnaruzheniya-vtorzheniy-v-suschestvuyuschih-informatsionnyh-sistemah

Исходными данными для его применения являются сведения из основной базы данных или ключевые слова сетевого трафика системы. К преимуществам сигнатурного анализа относят возможность его использования не только для сканирования на предмет выявления вредоносного программного обеспечения, но и для фильтрации сетевого трафика, к недостаткам применения – необходимость постоянного обновления баз банных и невозможность обнаружения новых угроз, сигнатуры которых нет в базе данных.

Суть анализа аномальной сетевой активности состоит в сравнении процесса функционирования КИИ с эталонной моделью его поведения, при условии допустимой вероятности ложных срабатываний. Примером аномалии может служить существенное повышение вычислительной активности, обращение к сторонним базам данных, отказ работы с пользовательским интерфейсом, блокировка компьютера, несвойственные операции, нестандартная реакция на входящую информацию и так далее [7,12,20].

Анализ поведения рабочих станций предполагает сравнение текущей активности с эталонной моделью при помощи специальных агентов. Если выявляется несоответствие поведения КИИ с эталонной моделью (с учетом априори заданной погрешности), то программное средство запрещается к реализации, а входящая информация блокируется. Здесь учитывается расширение области допусков информативного параметра: $\omega \in \Omega \to \omega_Z \in \Omega_Z$. Новая область определения Ω_Z ограничивается нечеткими границами, которые определяются не только свойствами деструктивного информационного воздействия, но и важностью КИИ и управляемого ею ВЭИО. Благодаря общему подходу алгоритмы поведенческого анализа способны решать специфические задачи и позволяют усовершенствовать системы безопасности КИИ [22]: определять аккаунты пользователей и конечных станций для включения их в перечень скомпрометированных («черный список»), предотвращать инсайдерские угрозы, проводить аудит прав доступа и так далее.

Наиболее перспективным методом обнаружения целевых атак является эвристический анализ, который относится к разновидности итеративных методов, основанных на прогнозировании и предположении, а не на фиксированном алгоритме. Главный принцип эвристического анализа основывается на предположении об осуществлении атаки, в нем отсутствуют жестко заданные правила и эталоны для проверки. Эвристический анализ включает использование нечетких и неконкретизированных методов обнаружения для поиска новых и неизвестных вредоносных программ: код файла или другого объекта проверяется на наличие подозрительных инструкций. Эвристические методы, применяемые в КИИ в рамках марковско-параметрического моделирования, сочетают в себе элементы сигнатурного анализа и выявление подозрительных действий со стороны внешних объектов или программного обеспечения[11]. Ряд эвристических методов обнаружения целевых атак предполагает поиск вирусов, похожих на известные. В системах обнаружения учитывается частичное совпадение исследуемых сигнатур с размещенными в базах. Эвристический анализ дает оценку вероятности обнаружения целевой атаки. Он предполагает, что новые вирусы по своему поведению схожи с уже ранее известными, поэтому сканирование всех файлов и объектов проводится на предмет определения выявленных сигнатур, имеющих сходство с уже известными.

Поиск объектов и программного обеспечения, выполняющих подозрительные действия, предполагает поиск действий, совершаемых в вычислительной составляющей КИИ, например, добавление новых файлов или регистров, изменение прав доступа, модификацию реестров, повышение привилегий учетных записей, открытие порта и другие. Каждое отдельно взятое действие может не вызывать подозрений на деструктивное воздействие, но их совокупность свидетельствует о подготовке целевой атаки. Такие программы или объекты переводятся в разряд подозрительных, для КИИ это означает, что необходимо провести комплекс мероприятий по оценке потенциальной опасности реализуемых алгоритмов.

Успешная и эффективная реализация комбинированного анализа по обнаружению целевых атак требует выполнения специфических вспомогательных функций. Функция обновления обеспечивает постоянное автоматическое пополнение базы данных сигнатур вредоносного программного обеспечения из всех известных источников. Функция автоматической настройки взаимодействия пользователя с программой управления КИИ необходима для доведения до оператора текущей обстановки и рекомендаций по противодействию целевой атаке. Наряду с функциями обнаружения целевых атак и связанных с этим мероприятий (запуск сканирования, обращение к базе сигнатур, проверка статуса зараженного файла или объекта, доступ к отчетам), КИИ обеспечивает пользователя

11 Эвристический анализ [Электронный ресурс] – Режим доступа https://encyclopedia.kaspersky.ru/glossary/heuristic-analysis/

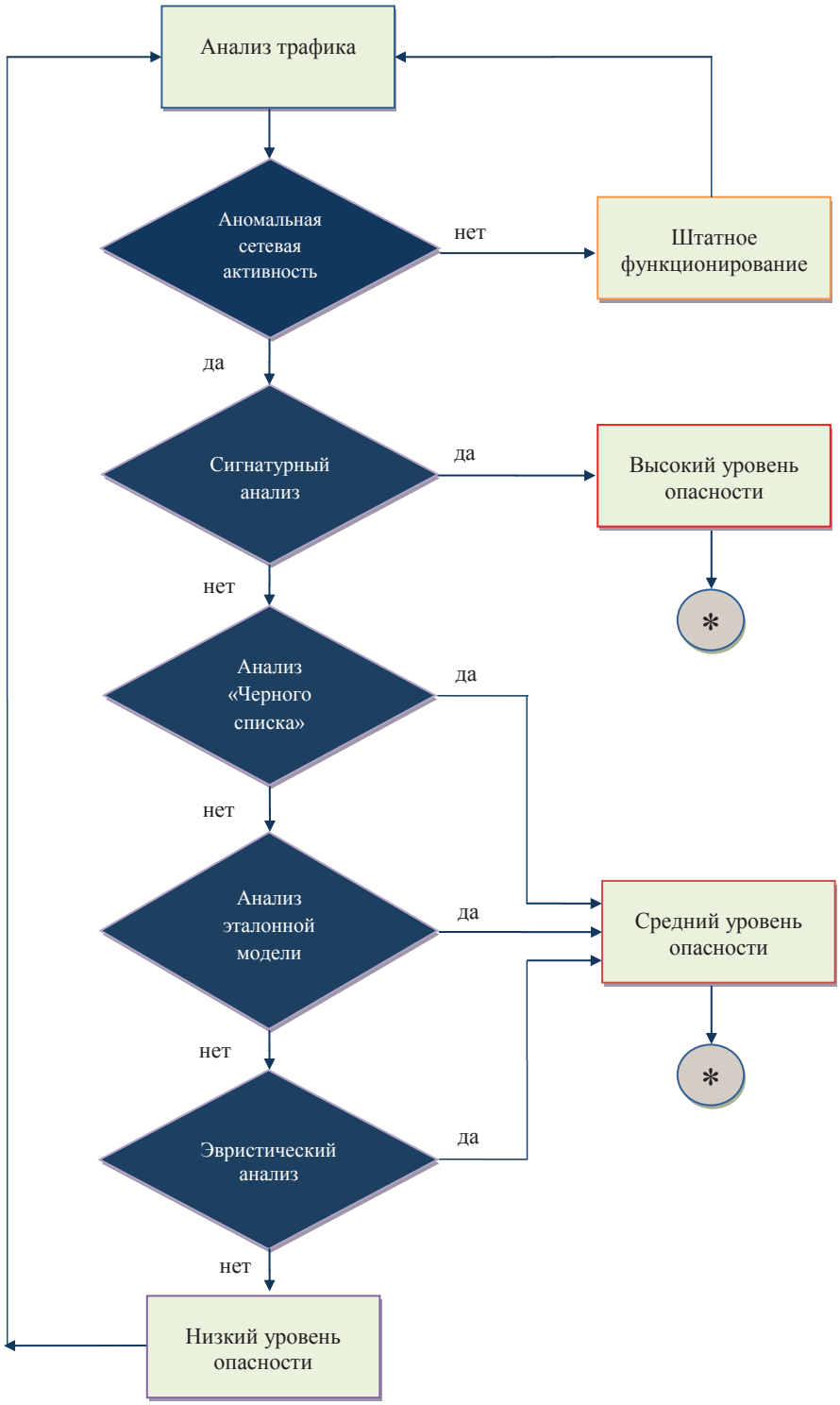

Рис. 2. Алгоритм режима нештатной эксплуатации КИИ

(оператора) рекомендациями по формированию управления [2,22,23]. Функция обеспечения реализует интеграцию классического метода эвристического анализа в марковско-параметрическую модель КИИ.

Несмотря на имеющиеся недостатки эвристического анализа, связанные с возможностью ложного определения деструктивного воздействия в поступающей информации и дополнительным расходом ресурсов вычислительной системы, он обладает способностью обнаруживать любое несанкционированное действие, которым проявляет себя ранее неизвестный вид программно-математического воздействия.

Таким образом, для обнаружения и защиты от целевых атак в КИИ могут использоваться все возможные методы, последним из которых должен стать эвристический анализ

Известно, что снижение в допустимых пределах качества функционирования КИИ при деструктивном информационном воздействии позволяет продолжать его эксплуатацию в течение некоторого времени. Это время используется для отражения целевой атаки, предотвращения ее распространения, ликвидации последствий, оценки опасности атаки для конкретной КИИ в конкретных условиях, выработки рекомендаций и формированию адекватных управляющих воздействий. В случае, если атака оказалась результативной, а ее последствия могут привести к аварии, катастрофе или неприемлемому ущербу от продолжения функционирования ВЭИО, управляющая КИИ вырабатывает решение на плановую его остановку. Анализ структурной схемы, приведенной на рисунке 1, показывает, что алгоритм функционирования КИИ в режиме нештатной эксплуатации необходимо дополнить алгоритмом обнаружения целевых атак.

4. Алгоритм обнаружения целевых атак и режима нештатной эксплуатации КИИ

Алгоритм режима нештатной эксплуатации КИИ на третьем периоде эксплуатации представлен на рис. 2.

На входе КИИ осуществляется анализ всей информации, как циркулирующей внутри системы «КИИ — ВЭИО», так и поступающей извне в рамках информационного взаимодействия с внешними ресурсами. При этом компьютерная атака, признаки которой имеются в базах, определяется методами сигнатурного анализа, а выявление целевой атаки осуществляется в соответствии с представленным алгоритмом.

Проводимый анализ направлен на выявление аномалий в поступающем трафике, отклонений от эталонной модели, проблемных событий в работе элементов КИИ, в частности в работе вычислительной составляющей автоматизированной системы управления технологическими и производственными процессами, как одного из элементов КИИ [22,23]. При отсутствии отклонений продолжается штатное функционирование КИИ.

Если же отклонения обнаружены, проводится проверка адресантов поступившей информации и стандартный сигнатурный анализ. Обнаружение в трафике адресов из «черного списка» или известных сигнатур переводит КИИ в режим нештатной эксплуатации. Объект КИИ осуществляет оценку свойств и характеристик деструктивного воздействия и в зависимости от уровня опасности принимает решение о дальнейшей эксплуатации в соответствии с алгоритмом, приведенным в [10].

Отсутствие подозрительных адресов и сигнатур в базе данных еще не гарантирует отсутствие деструктивного информационного воздействия на КИИ. Возможно, воздействие осуществляется в виде целевой атаки, параметры которой уникальны и разработаны под конкретную КИИ. В этом случае система переходит в режим эвристического анализа. Если эвристический анализ не выявил признаков деструктивного воздействия, принимается решение о продолжении штатной эксплуатации, алгоритмический цикл повторяется в условиях усиления наблюдения к работе КИИ. Обнаружение признаков деструктивного воздействия переводит КИИ в режим нештатной эксплуатации, основным содержанием которого будет эвристическая оценка неизвестного воздействия.

Оценка свойств и характеристик неизвестного воздействия проводится всеми доступными методами. Можно использовать метод аналогий, метод частичного совпадения сигнатур, различные экспертные методы, методы имитационного моделирования и другие. Гарантированное продолжение эксплуатации предполагает пессимистическую оценку воздействия и основных параметров функционирования КИИ.

Итогом работы КИИ по выявлению и противодействию целевой атаке в рамках марковско-параметрической модели будет расширение области определения параметра $\omega \in \Omega \to \omega_Z \in \Omega_Z$, изменение допусков $\omega_{Z\max}$ и $\omega_{Z\min}$, занесение информации о новой атаке (адреса, сигнатуры, другие признаки) в базу данных и базу знаний КИИ.

Схема алгоритма оценки свойств и характеристик деструктивного воздействия (целевой атаки) приведена на рис. 3.

Предварительная оценка опасности деструктивного информационного воздействия проводится параллельно с оценкой его свойств и характеристик в соответствии с представленной схемой в зависимости от этапа выявления компьютерной атаки, итоговая – после получения значения информативного параметра $\omega_Z(t) \in \Omega_Z$. По аналогии с [10,12] проводится сравнение свойств и характеристик целевой атаки $\omega_z(t)$ с допусками, значения которых могут изменяться по мере накопления сведений о состоянии КИИ в условиях деструктивного воздействия.

Рис. 3 — Схема алгоритма оценки деструктивного воздействия

Ситуация $\omega_1(t) \le \omega_{1\min}(t)$ или $\omega_Z(t) \le \omega_{Z\min}(t)$ (низкий уровень воздействия) предполагает продолжение штатной эксплуатации при условии принятия дополнительных мер по мониторингу складывающейся обстановки. Дополнительно проводится оперативная оценка состояния КИИ для определения эффективности принимаемых мер, осуществляются отдельные мероприятия по его нейтрализации целевой атаки. КИИ продолжает управление значимой системой в штатном режиме.

Превышение уровня воздействия выше допустимого $\omega_1(t) \ge \omega_{1\max}(t)$ или $\omega_Z(t) \ge \omega_{Z\max}(t)$ (высокий уровень воздействия) требует немедленного прекращения эксплуатации КИИ и отключения от управляемого ею объекта (перевода управления в ручной режим). В этой ситуации КИИ отключается от сетей общего пользования, проводятся работы по ликвидации последствий целевой атаки и восстановлению показателей функционирования КИИ.

Промежуточное значение вектора параметра $\omega_{1\min}(t) < \omega_Z(t) < \omega_{1\max}(t)$ или $\omega_{Zmxin}(t) < \omega_Z(t) < \omega_{Z\max}(t)$ предполагает оперативную оценку возможности продолжения эксплуатации, выработку мер по устранению деструктивного воздействия, определение интервала времени, в течение которого возможна реализация выработанных рекомендаций по нейтрализации деструктивного воздействия. Функционирование КИИ при этом не прекращается. После вычисления основных стохастических характеристик КИИ – вероятности нахождения ее в работоспособном состоянии и времени нахождения исследуемых параметров в границах допустимой области – вырабатываются рекомендации и формируются управляющие воздействия на ВЭИО.

Предложенная модель с интегрированной в ее состав системой обнаружения целевых атак может быть использована при разработке перспективных КИИ, обеспечивающих повышение устойчивости КИИ и оперативное гарантированное противодействие деструктивным информационным воздействиям.

Заключение

В данной работе на основе анализа функционирования КИИ в условиях актуальной угрозы деструктивного информационного воздействия обоснована необходимость модификации марковско-параметрической модели объекта в направлении расширения возможностей по выявлению целевых атак и противодействию им.

Проведен анализ свойств целевых атак и особенностей их воздействия на объекты КИИ, реализующие управление технологическими и производственными процессами. Оценка существующих и перспективных методов выявления целевых атак позволила синтезировать алгоритм их обнаружения на базе сочетания различных методов с приоритетом эвристического анализа. Интеграция синтезированного алгоритма в ранее разработанную марковско-параметрическую модель КИИ расширяет ее возможности по нейтрализации деструктивного информационного воздействия. Предварительную оценку опасности деструктивного информационного воздействия и выработку рекомендаций по нейтрализации предлагается проводить параллельно с оценкой его свойств и характеристик.

Основные результаты работы могут быть использованы при создании перспективных объектов КИИ с повышенной устойчивостью к целевым компьютерным атакам и безопасностью ее функционирования в сферах здравоохранения, науки, транспорта, связи, энергетики, и других.

Литература

1. Госькова Д.А., Массель А.Г. Технология анализа киберугроз и оценка рисков кибербезопасности критической инфраструктуры // Вопросы кибербезопасности. 2019. №2. С. 42-49. DOI:10.21681/2311-3456-2019-2-42-49.
2. Скрыль С.В., Гайфулин В.В., Домрачев Д.В., Сычев В.М., Грачёва Ю.В. Актуальные вопросы проблематики оценки угроз компьютерных атак на информационные ресурсы значимых объектов критической информационной инфраструктуры // Безопасность информационных технологий. 2021. Т. 28. № 1. С. 84-94. DOI: 10.26583/bit.2021.1.07.
3. Грачков И.А. Информационная безопасность АСУ ТП: возможные вектора атаки и методы защиты // Безопасность информационных технологий. 2018. Т. 25. № 1. С. 90-98.
4. Кондаков С.Е., Рудь И.С. Модель процесса проведения компьютерных атак с использованием специальных информационных воздействий // Вопросы кибербезопасности. 2021. №5. С. 12-20. DOI: 10.21681/2311-3456-2021-5-12-20.
5. Таныгин М.О, Будникова Ю.А., БулгаковА.С., Марченко М.А. Модель оценки ущерба от инцидентов информационной безопасности. // Безопасность информационных технологий. 2021. № 2. стр. 98-106.
6. Васильев В.И., Кириллова А.Д, Вульфин А.М. Когнитивное моделирование вектора кибератак на основе меташаблонов Capec // Вопросы кибербезопасности. 2021. № 2. С. 2-16. DOI: 10.21681/2311-3456-2021-2-2-16.
7. Краснов А.Е., Мосолов А.С., Феоктистова Н.А. Оценивание устойчивости критических информационных инфраструктур к угрозам информационной безопасности // Безопасность информационных технологий. 2021. Т. 28. № 1.С. 106-120. DOI: 10.26583/bit.2021.1.09.
8. Максимова Е.А. Когнитивное моделирование деструктивных злоумышленных воздействий на объектах критической информационной инфраструктуры // Труды учебных заведений связи. 2020. Т. 6. № 4. С. 91-103. DOI:10.31854/1813-324X-2020-6-4-91-103.
9. Острейковский В.А., Лысенкова С.А. Концепция современных подходов к уровням описания процессов старения структурно и функционально сложных критически важных систем с длительными сроками активного существования // Надежность и качество сложных систем. 2021. № 3. С. 5-12. DOI: 10.21685/2307-4205-2021-3-1.
10. Кубарев А.В., Лапсарь А.П., Федорова Я.В. Повышение безопасности эксплуатации значимых объектов критической инфраструктуры с использованием параметрических моделей эволюции // Вопросы кибербезопасности. 2020. № 1. С. 8-17. DOI:10.21681/2311-3456-2020-1-8-17.
11. Воронин Е.А., Дарьина А.Н., Дивеев А.И., Прокопьев И.В., Юрков Н.К. У истоков теории надежности сложных систем // Надежность и качество сложных систем. № 1. 2020. С. 3-4.
12. Кубарев А.В., Лапсарь А.П., Асютиков А.А. Синтез модели объекта критической информационной инфраструктуры для безопасного функционирования технической системы в условиях деструктивного информационного воздействия // Вопросы кибербезопасности. 2020. №6. С. 48-56. DOI: 10.681/2311-3456-2020-6-48-56.
13. Бачманов Д. А. Исследование вопросов совершенствования систем защиты от DDos-атак на основе комплексного анализа современных механизмов противодействия / Бачманов Д. А., Очередько А. Р., Путято М. М., Макарян А. С. // Прикаспийский журнал: управление и высокие технологии. – 2021. – №1. – С. 63-74.
14. Подкопаев А.В., Подкопаев И.А. Централизованный адаптивный алгоритм оценки безотказности сложных технических систем различной энтропии // Надежность и качество сложных систем. № 1. 2020. С. 49-56. DOI: 10.21685/2307-4205-2020-1-6.
15. Орлова Д.Е. Комплекс программ для решения задач моделирования, оптимизации и оценки устойчивости комплексной безопасности объектов критического применения // Моделирование, оптимизация и информационные технологии. 2020. Т. 8. № 1. С. 43-44. DOI: 10.26102/2310-6018/2020.28.1.036.
16. Андрюхин Е.В., Ридли М.К., Правиков Д.И., Прогнозирование сбоев и отказов в распределенных системах управления на основе моделей прогнозирования временных рядов // Вопросы кибербезопасности. 2019. № 3. С. 24-32. DOI:10.21681/2311-3456-2019-3-24-32.
17. Лифшиц И.И., Фаткиева Р.Р. Модель интегрированной системы менеджмента для обеспечения безопасности сложных объектов // Вопросы кибербезопасности. 2018. №1. С. 64-71. DOI:10.21681/2311-3456-2018-1-64-71.
18. Панкин А.М. Основные вопросы методологии диагностирования сложных технических объектов // Надежность и качество сложных систем. № 2. 2021. С. 62-69. DOI: 10.21685/2307-4205-2021-2-6.
19. Северцев Н.А., Дарьина А.Н. Применение критериев подобия при ресурсной отработке сложных технических систем и изделий // Надежность и качество сложных систем. № 4. 2020. С. 5-14. DOI: 10.21685/2307-4205-2020-4-1.
20. Лаврова Д.С., Зегжда Д.П., Зайцева Е.А Моделирование сетевой инфраструктуры сложных объектов для решения задачи противодействия кибератакам // Вопросы кибербезопасности. 2019. №2. С. 13-20. DOI: 10.21681/2311-3456-2019-2-13-20.

21. Салкуцан А.А., Гавдан Г.П., Полуянов А.А. Методика определения критических процессов на объектах информационной инфраструктуры // Безопасность информационных технологий. 2020. Т. 27. № 2. С. 18-34. DOI: 10.26583/bit.2020.2.02.
22. Гришко А.К., Лысенко А.В., Моисеев С.А. Прогнозирование и оптимизация управления процессов проектирования сложных технических систем в масштабе реального времени // Надежность и качество сложных систем. № 1. 2018. С. 40-45. DOI: 10.21685/2307-4205-2018-1-5.
23. Северцев Н.А., Бецков А.В., Дарьина А.Н. Методы и модели создания автоматизированных средств контроля для повышения безопасности функционирования технических систем // Надежность и качество сложных систем. № 2. 2019. С. 19-26. DOI: 10.21685/2307-4205-2019-2-3.

ENSURING THE RESISTANCE OF CRITICAL INFORMATION INFRASTRUCTURE OBJECTS TO ADVANCED PERSISTENT THREATS

***Lapsar' A.P.*[12] *, Nazaryan S.A.*[13]*, Vladimirova A.I.*[14]**

The purpose of the study: *to improve security of significant objects of critical information infrastructure in conditions of destructive information impact, implemented in the form of advanced persistent threat (APT).*

Methods: *comparative analysis of destructive information impact within the framework of a systematic approach; Markov theory of evolutionary processes; synergetics.*

Results: *the authors carried out analysis of APT properties and their impact on objects of critical information infrastructure. To identify APTs, the use of a combination of various detection methods with the priority of heuristic analysis is substantiated. A scheme has been developed for the implementation of the method for assessing the state of an object of a critical information infrastructure based on a modified Markov-parametric model with a system for detecting computer attacks integrated into its structure. The preliminary assessment of computer attacks danger level as well as development of recommendations for their neutralization simultaneously with conducting the assessment of the properties and characteristics of destructive information impact are proposed.*

Keywords: *destructive information impact, APT, Markov parameterized model, state assessment, object of critical information infrastructure.*

References

1. Gos'kova D.A., Massel' A.G. Tekhnologiya analiza kiberugroz i ocenka riskov kiberbezopasnosti kriticheskoj infrastruktury // Voprosy kiberbezopasnosti [Cybersecurity issues]. 2019. №2. S. 42-49. DOI:10.21681/2311-3456-2019-2-42-49
2. Skryl' S.V., Gajfulin V.V., Domrachev D.V., Sychev V.M., Grachyova YU.V. Aktual'nye voprosy problematiki ocenki ugroz komp'yuternyh atak na informacionnye resursy znachimyh ob"ektov kriticheskoj informacionnoj infrastruktury // Bezopasnost' informacionnyh tekhnologij. 2021. T. 28. № 1. S. 84-94. DOI: 10.26583/bit.2021.1.07
3. Grachkov I.A. Informacionnaya bezopasnost' ASU TP: vozmozhnye vektora ataki i metody zashchity // Bezopasnost' informacionnyh tekhnologij. 2018. T. 25. № 1. S. 90-98.
4. Kondakov S.E., Rud' I.S. Model' processa provedeniya komp'yuternyh atak s ispol'zovaniem special'nyh informacionnyh vozdejstvij // Voprosy kiberbezopasnosti [Cybersecurity issues]. 2021. №5. S. 12-20. DOI: 10.21681/2311-3456-2021-5-12-20.
5. Tanygin M.O, Budnikova YU.A., BulgakovA.S., Marchenko M.A. Model' ocenki ushcherba ot incidentov informacionnoj bezopasnosti. // Bezopasnost' informacionnyh tekhnologij. 2021. № 2. str. 98-106.

12 Alexey Lapsar, Ph.D., Associate Professor, Deputy Head of the Department of the FSTEK of Russia (Federal service for Technical and Export control) for the Southern and North Caucasian Federal Districts, Rostov-on-Don, Russia, E-mail: lapsarap1958@mail.ru

13 Sergey Nazaryan, Associate Professor of Information technology and Information security Chair, Rostov State University of Economics (RINH), Rostov-on-Don, Russia. E-mail: serj_nazaryan@mail.ru

14 Alisa Vladimirova, Master student, Rostov State University of Economics (RINH), Rostov-on-Don, Russia. E-mail: alisa.v@mail.ru.

6. Vasil'ev V.I., Kirillova A.D, Vul'fin A.M. Kognitivnoe modelirovanie vektora kiberatak na osnove metashablonov Sapec // Voprosy kiberbezopasnosti [Cybersecurity issues]. 2021. № 2. S. 2-16. DOI: 10.21681/2311-3456-2021-2-2-16.
7. Krasnov A.E., Mosolov A.S., Feoktistova N.A. Ocenivanie ustojchivosti kriticheskih informacionnyh infrastruktur k ugrozam informacionnoj bezopasnosti // Bezopasnost' informacionnyh tekhnologij. 2021. T. 28. № 1.S. 106-120. DOI: 10.26583/bit.2021.1.09.
8. Maksimova E.A. Kognitivnoe modelirovanie destruktivnyh zloumyshlennyh vozdejstvij na ob"ektah kriticheskoj informacionnoj infrastruktury // Trudy uchebnyh zavedenij svyazi. 2020. T. 6. № 4. S. 91-103. DOI:10.31854/1813-324X-2020-6-4-91-103.
9. Ostrejkovskij V.A., Lysenkova S.A. Koncepciya sovremennyh podhodov k urovnyam opisaniya processov stareniya strukturno i funkcional'no slozhnyh kriticheski vazhnyh sistem s dlitel'nymi srokami aktivnogo sushchestvovaniya // Nadezhnost' i kachestvo slozhnyh sistem. 2021. № 3. S. 5-12. DOI: 10.21685/2307-4205-2021-3-1.
10. Kubarev A.V., Lapsar' A.P., Fedorova YA.V. Povyshenie bezopasnosti ekspluatacii znachimyh ob"ektov kriticheskoj infrastruktury s ispol'zovaniem parametricheskih modelej evolyucii // Voprosy kiberbezopasnosti [Cybersecurity issues]. 2020. № 1. S. 8-17. DOI:10.21681/2311-3456-2020-1-8-17.
11. Voronin E.A., Dar'ina A.N., Diveev A.I., Prokop'ev I.V., YUrkov N.K. U istokov teorii nadezhnosti slozhnyh sistem // Nadezhnost' i kachestvo slozhnyh sistem. № 1. 2020. S. 3-4.
12. Kubarev A.V., Lapsar' A.P., Asyutikov A.A. Sintez modeli ob"ekta kriticheskoj informacionnoj infrastruktury dlya bezopasnogo funkcionirovaniya tekhnicheskoj sistemy v usloviyah destruktivnogo informacionnogo vozdejstviya // Voprosy kiberbezopasnosti [Cybersecurity issues]. 2020. №6. S. 48-56. DOI: 10.681/2311-3456-2020-6-48-56.
13. Bachmanov D. A. Issledovanie voprosov sovershenstvovaniya sistem zashchity ot DDos-atak na osnove kompleksnogo analiza sovremennyh mekhanizmov protivodejstviya / Bachmanov D. A., Ochered'ko A. R., Putyato M. M., Makaryan A. S. // Prikaspijskij zhurnal: upravlenie i vysokie tekhnologii. – 2021. – №1. – S. 63-74.
14. Podkopaev A.V., Podkopaev I.A. Centralizovannyj adaptivnyj algoritm ocenki bezotkaznosti slozhnyh tekhnicheskih sistem razlichnoj entropii // Nadezhnost' i kachestvo slozhnyh sistem. № 1. 2020. S. 49-56. DOI: 10.21685/2307-4205-2020-1-6.
15. Orlova D.E. Kompleks programm dlya resheniya zadach modelirovaniya, optimizacii i ocenki ustojchivosti kompleksnoj bezopasnosti ob"ektov kriticheskogo primeneniya // Modelirovanie, optimizaciya i informacionnye tekhnologii. 2020. T. 8. № 1. S. 43-44. DOI: 10.26102/2310-6018/2020.28.1.036
16. Andryuhin E.V., Ridli M.K., Pravikov D.I., Prognozirovanie sboev i otkazov v raspredelennyh sistemah upravleniya na osnove modelej prognozirovaniya vremennyh ryadov // Voprosy kiberbezopasnosti [Cybersecurity issues]. 2019. № 3. S. 24-32. DOI:10.21681/2311-3456-2019-3-24-32.
17. Lifshic I.I., Fatkieva R.R. Model' integrirovannoj sistemy menedzhmenta dlya obespecheniya bezopasnosti slozhnyh ob"ektov // Voprosy kiberbezopasnosti [Cybersecurity issues]. 2018. №1. S. 64-71. DOI:10.21681/2311-3456-2018-1-64-71.
18. Pankin A.M. Osnovnye voprosy metodologii diagnostirovaniya slozhnyh tekhnicheskih ob"ektov // Nadezhnost' i kachestvo slozhnyh sistem. № 2. 2021. S. 62-69. DOI: 10.21685/2307-4205-2021-2-6.
19. Severcev N.A., Dar'ina A.N. Primenenie kriteriev podobiya pri resursnoj otrabotke slozhnyh tekhnicheskih sistem i izdelij // Nadezhnost' i kachestvo slozhnyh sistem. № 4. 2020. S. 5-14. DOI: 10.21685/2307-4205-2020-4-1.
20. Lavrova D.S., Zegzhda D.P., Zajceva E.A Modelirovanie setevoj infrastruktury slozhnyh ob"ektov dlya resheniya zadachi protivodejstviya kiberatakam // Voprosy kiberbezopasnosti [Cybersecurity issues]. 2019. №2. S. 13-20. DOI: 10.21681/2311-3456-2019-2-13-20.
21. Salkucan A.A., Gavdan G.P., Poluyanov A.A. Metodika opredeleniya kriticheskih processov na ob"ektah informacionnoj infrastruktury // Bezopasnost' informacionnyh tekhnologij. 2020. T. 27. № 2. S. 18-34. DOI: 10.26583/bit.2020.2.02.
22. Grishko A.K., Lysenko A.V., Moiseev S.A. Prognozirovanie i optimizaciya upravleniya processov proektirovaniya slozhnyh tekhnicheskih sistem v masshtabe real'nogo vremeni // Nadezhnost' i kachestvo slozhnyh sistem. № 1. 2018. S. 40-45. DOI: 10.21685/2307-4205-2018-1-5.
23. Severcev N.A., Beckov A.V., Dar'ina A.N. Metody i modeli sozdaniya avtomatizirovannyh sredstv kontrolya dlya povysheniya bezopasnosti funkcionirovaniya tekhnicheskih sistem // Nadezhnost' i kachestvo slozhnyh sistem. № 2. 2019. S. 19-26. DOI: 10.21685/2307-4205-2019-2-3.