Инженерный вестник Дона, №11 (2024)
ivdon.ru/ru/magazine/archive/n11y2024/9646

Риск-устойчивость центров мониторинга информационной безопасности и ее моделирование

А. В. Пономарев

Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация.

Аннотация: Цель статьи – исследование информационной безопасности критических параметров процессов ИТ-инфраструктуры организации, ее цифровой инфраструктуры с помощью Центров мониторинга безопасности. Акцентируются такие факторы рисков, как адаптивность, устойчивость в среднем и длительном периоде, влияние неопределенностей («белого шума»). Кроме системного анализа-синтеза в работе используются методы математического (имитационного, операторного) моделирования, вычислительной математики и статистики. На основе проведенного анализа и синтеза в работе получены следующие основные результаты: 1) проведена классификация воздействий различных атак на распределенную инфраструктуру; 2) предложены схема, мультипликативная модель интегральных взаимодействий защитных мер и интегральная мера защищенности; 3) разработан алгоритм идентификации построенной мультипликативной модели на основе критерия наименьших квадратов, как по совокупности факторов, так и по классам рисков; 4) приведен пример операторного уравнения с учетом случайного шума в системе. Научно-практическая ценность работы: результаты могут быть использованы для оценки защищенности системы и снижения рисков целевых атак, ущерба от них. Кроме этого, предложенные схемы позволят облегчить ситуационное моделирование по обнаружению риск-ситуаций и оценки ущерба от их реализации
Ключевые слова: оценка, устойчивость, зрелость, центр информационной безопасности, мониторинг, риск, управление.

Введение. Постановка задачи

Цель мониторинга – получение оценок, которые позволяют корректировать выводы по риск-безопасности и сделать более эффективным мониторинг и повысить его инновационный потенциал. Мониторинг требует релевантной обработки и интеллектуального принятия решений, оперативного отклика на реальную ситуацию, особенно, на критических участках системы, в нештатных ситуациях.

По статистике каждые 14 секунд происходит атака программы-вымогателя («шифровщика», «шифровальщика»), а усредненная длительность нахождения ее в системе (сети) составляет 4 час.

Защищенность цифровой инфраструктуры – актуальная проблема в условиях разнообразных рисков и уязвимостей системы [1–3]. В информационной распределенной системе (далее, система) чаще организуются целевые атаки на ИТ-инфраструктуру, цифровую экосистему (далее, просто «экосистема»). Такие атаки направлены на ключевые подсистемы, в частности, управления. Это критически важные и чувствительные к деструктивным воздействиям информационные подсистемы.

Вредоносный код способен использоваться при доступе и к закрытой корпоративной информации, следует контролировать пространство доступа и вне клиентской части. Например, DLP-система позволяет идентифицировать активность и отслеживать трафик, «следы», вести протоколирование.

Актуально стало формировать специальные Центры мониторинга и управления безопасностью (Security Operation Center, SOC), которые в цифровой инфраструктуре (экосистеме) корпорации является важной подсистемой взаимосвязанных проектов на основе процессного подхода. Использует языки, модели поиска, идентификации и устойчивой нейтрализации атак на экосистему.

Актуальны ключевые задачи эффективного мониторинга – поиск мониторинговой последовательности и инфраструктуры для результативного мониторинга, а также оценка ресурсов, необходимых для него, оценка событий и всей системы по уязвимости, недопущение атак (закрытие точек доступа в инфраструктуру).

Моделирование воздействия рисков – это сложная и многокритериальная, многофакторная задача, которая требует учета неопределенности, стохастичности, оценки возможного ущерба [4,5].

Целью статьи является системный анализ факторов и критериев оценки зрелости SOC, их структурирование, исследование перспектив

результативного ситуационного (имитационного) моделирования кибератак. Такая задача ставится и исследуется в статье при определенных условиях на факторы устойчивости.

Методология

В проблеме прогнозирования устойчивости и зрелости SOC-центра сложно построить формализованную и верифицируемую модель, поэтому важны эвристические, нейросетевые, когнитивные, мультиагентные и имитационные подходы [6,7]. Но для всех инструментальных подходов необходимы формализуемые, структурируемые меры эффективности и оценочные метрики.

При отсутствии универсальных моделей оценки уровня мониторинга риск-устойчивости, применяемые при исследовании методы должны быть:

1) достоверными и воспроизводимыми;
2) охватывающими последовательно весь жизненный цикл мониторинга;
3) универсальными по учитываемым показателям и их ранжированию (шкалированию);
4) адаптивными к потребностям управления безопасностью организации;
5) не допускающими снижения показателей устойчивости в «полосе» допусков (спецификаций), например, шаблонов Capec [8];
6) при атаке SOC не реагирует снижением показателей устойчивости в длительном, недопустимом периоде и обеспечивает устойчивое управление при отсутствии атаки.

Используемые в исследованиях методы системного и когнитивного анализа, идентификации моделей безопасности направлены на устойчивость траектории функционирования SOC, релевантный анализ уязвимостей и ситуационное моделирование. Например, учитывается динамическое состояние в системе, а также неопределенности и шумы класса «Белый шум» в данных, потоках и транзакциях экосистемы.

Устойчивость мониторинга и риск-анализ уязвимостей информационной сети

В распределенной информационной сети следует учитывать динамическое состояние, а также «подвижность» событий и их структурную активность. Например, в атаках класса MitM (Man-in-the-Middle) [9], сложность организации и неопределенности в мониторинговых данных вносится самой структурой, а также сопутствующими шумами при обработке потоков данных.

Поэтому целевые атаки готовят заранее, используя анализ уязвимостей, адаптируя под них меры. Популярно стало применение метода хаос-инжиниринга, хаос-тестирования и иные. Уязвимы система файлов, архитектура сети, сама вычислительная активность и др.

Релевантный SOC-мониторинг и устойчивая безопасность – единство функциональности и эффективности, которое реализуется на принципах:

1) идентификации и локализации уязвимостей;
2) разработки полных рекомендаций для персонала;
3) аудита рисков (атак) с максимальной диагностикой и охватом клиентской, информационной, функциональной подсистемы;
4) регулярного мониторинга риск-устойчивости и безопасности на полном цикле от спецификаций до проектирования эксплуатационных возможностей.

Здесь необходимо релевантное ситуационное моделирование. Часто разрабатывается и специальная стратегия проникновения в систему, специальное ПО, например, контроля и аналитики событий и учетных записей. Уязвимы файловая система, штатная архитектура сети, данные БД, облачные и туманные, вычислительная активность и др.

Сигнатурный анализ позволяет выявлять аномалию, готовиться к целевой атаке и настраиваться к «встрече» с ней. Машинное обучение для

соответствующей нейросистемы позволит сформировать классы деструктивных действий. Они позволят автоматически формировать профили, эталоны (модели) осуществления атак и аудита системы. Более сложная задача – поиск точек проникновения в систему.

«Цифровые двойники» атак (атакуемых ситуаций, событий) позволяют идентифицировать новые атаки на уровне критически защищенного уровня управления с необходимой их нейтрализацией.

Источниками рисков в распределенной организации, ее инфраструктуре могут являться [10]:

1) удаленное администрирование;
2) слабозащищенные пароли и протоколы;
3) сбои автоматического конфигурирования;
4) недостаточно качественно проведенный аудит уязвимостей;
5) некомпетентность персонала (пользователя);
6) «человеческий фактор» и др.

Обрабатываемый системой безопасности поток данных – это, как правило, пространственно-временный ряд со случайными параметрами. Необходимо, например, выделить вредоносные пространственно-временные сигналы потока. Применяются различные модели и адаптивная схема для моделирования (рис.1).

Задачи безопасности решаются различными методами, например, преобразования Фурье или вейвлет. Метод Фурье базируется на сосредоточенной в малой окрестности точки функции, резко убывающей до нуля при удалении (по времени, частоте). Метод вейвлет – на нулевом интегральном значении и применении сдвига по времени и масштабировании (растяжении или сжатии).

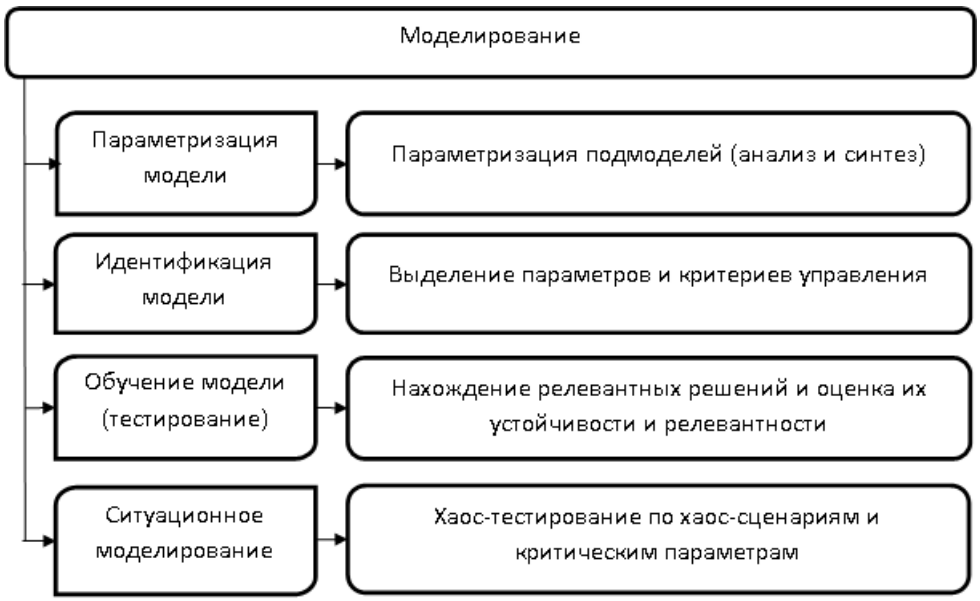

Рис. 1. Схема риск-моделирования (авторы)

Часто используют дискретное Фурье-преобразование, которое переводит сигналы из временной области в частотную, например, с помощью пакета MatLab – прямое преобразование:

$$y(k) = \sum_{i=1}^{n} x(i) e^{\frac{2\pi}{n(i-1)(k-1)}},$$

а также обратно:

$$\mathrm{x}(k) = \sum_{i=1}^{n} y(i) e^{\frac{-2\pi}{n(i-1)(k-1)}}.$$

С помощью этих преобразований можно эффективно и гибко оперировать с данными (временными и частотными), обнаруживать в них аномалии, а также выделять их из «шумов», помех.

В задаче моделирования устойчивости SOC-систем важно оценить степень и потенциал защищенности систем, опираясь на классы угроз и учитывая механизмы защиты. Класс защиты оценим индексом риска, например, размахом

$$R = R_{max} - R_{min},$$

где R_{max} – максимальный рейтинг защиты данных, R_{min} – минимальный рейтинг допуска пользователей.

Также важно идентифицировать момент вторжения и использования протокола (алгоритма) обслуживания искусственно сгенерированного потока задач, например, при DDoS-атаках.

Мультипликативная модель оценивания защищенности информационной сети и алгоритм ее идентификации

Предлагается мультипликативная модель интегральных взаимодействий защитных мер, взаимодействующих параллельно, с мерой (интегральным критерием) защищенности в виде:

$$F = F_0 \prod_{i=1}^{n} \left(\frac{x_i(t) - x_i^{max}}{x_i^{opt} - x_i^{min}} \right)^{\beta_i(t)} \left(\frac{x_i^{max} - x_i(t)}{x_i^{max} - x_i^{opt}} \right)^{-\beta_i(t) \frac{x_i^{max} - x_i^{opt}}{x_i^{opt} - x_i^{min}}},$$

где F_0 – оценка уровня защищенности в начальный момент времени (задается экспертами, статистически), n – число учитываемых факторов защиты, $x_i(t)$ – текущее, в момент t, значение фактора, x_i^{max}, x_i^{min}, x_i^{opt} – соответственно, максимальное, минимальное и оптимальное его значения, $\beta_i(t)$ – мера важности учета фактора i, его вклад в обеспечение непрерывной и устойчивой безопасности.

Коэффициенты $\beta_i(t)$, $i = 1,2,\dots,n$ подлежат идентификации: а) либо по совокупности факторов; б) либо по их кластерам (классам опасностей, например, MitM).

Параметры определяются на основе экспертно-эвристических и/или статистических данных на задаваемый период. Например, x_1 – количество (частота) сбоев аппаратуры, x_2 – количество ошибок персонала (уровень

«человеческого фактора»), x_3 – уровень инсайдерства, x_4 – фоновый шум в каналах, x_5 – степень тестирования ПО и др. Для x_i^{min}, x_i^{opt}, x_i^{max} можно использовать квартильные значения.

Алгоритм идентификации строится на основе метода наименьших квадратов, с использованием критерия (функционала) адекватности:

$$\Phi(\beta_1, \beta_2, \dots, \beta_n) = \sum_{i=1}^{n} (\ln F(t_i) - f_i)^2 \Rightarrow min,$$

где n – число рассматриваемых факторов защиты, f_i – данные мониторинга (аудита) безопасности (SOC).

Переходя к достаточным условиям достижения экстремума, а именно, к системе:

$$\frac{\partial \Phi}{\partial \beta_i} = 0, \;\; i = 1,2, \dots, n,$$

можно получить нормальную систему алгебраических уравнений, которая разрешима.

Например, при постоянных значениях β_i получаем систему линейных алгебраических уравнений, решаемых, например, методом квадратных корней (см. [11]) с использованием, в частности, математического пакета MathLab или аналогичного.

Идентифицированные параметры β_i $(i = 1,2, \dots, n)$ позволяют проводить прогноз защищенности системы по формуле:

$$F(t) = F_0 \exp \sum_{i=1}^{n} \beta_i \ln A_i(t),$$

где $A_i(t)$ – форма, определяемая входными параметрами F_0, x_i^{min}, x_i^{opt}, x_i^{max}, которые задаются экспертами или статистически.

В случае постоянных параметров β_i $(i = 1,2,\dots,n)$ и дискретной временной сетки t_k $(k = 1,2,\dots,m)$ получаем систему уравнений $(j = 1,2,\dots,n)$:

$$\beta_1 \sum_{k=1}^{m} lnA_{jk} lnA_{1k} + \beta_2 \sum_{k=1}^{m} lnA_{jk} lnA_{2k} + \cdots + \beta_n \sum_{k=1}^{m} lnA_{jk} lnA_{nk},$$

где коэффициенты имеют вид:

$$A_{ik} = \left(\frac{x_{ik} - x_k^{max}}{x_k^{opt} - x_k^{min}}\right)\left(\frac{x_k^{max} - x_{ik}}{x_k^{max} - x_k^{opt}}\right)^{-\frac{x_k^{max} - x_k^{opt}}{x_k^{opt} - x_k^{min}}},$$

$$x_{ik} = A_i(t_k).$$

Модель эта пригодна и для ранжирования систем по защищенности, причем уровни могут быть и количественными, и качественными. Например, уровень, обозначаемый как «0» соответствует полной (безусловной, абсолютной незащищенности), а обозначаемый как «1» – полной защищенности.

Основная сложность оценки защищенности для SOC заключается в сложности мониторинга (аудита) безопасности и влиянии «проклятья размерности». Поэтому предложенная выше сбалансированная система индикаторов и интегральная модель безопасности вместе с хорошо реализуемым алгоритмом идентификации позволит достаточно релевантно и адаптивно оценить защищенность системы.

Неклассические («мягкие») подходы к моделированию уровня защищенности и их возможности в многоуровневой системе защиты

Переход к «мягким» (Softskills) способам, моделям анализа и оценки защищенности – необходимость, вызванная усложнение атак, ростом их

количества. Для решения сложных и комплексных задач интеллектуального мониторинга безопасности сети привлекаются интеллектуальные платформы и технологии интерактивного анализа состояний и данных.

Поддержка распределенного мониторинга происходит по схеме: «пользователь – сеть – система – мониторинг – аналитик».

Для реализации схемы используются знания об объекте мониторинга *O* и системе мониторинга *S*:

$$O=<Q, R, P, F>, \quad S=<A, K, M, D>,$$

1) $Q = \{Q_1, Q_2, \dots, Q_n\}$ – совокупность спецификаций *O*;
2) $R = \{R_{11}, R_{12}, \dots, R_{nn}\}$ – совокупность бинарных отношений *O*;
3) $P = \{P_1, P_2, \dots, P_n\}$ – совокупность определяющих (разнородных) свойств *O;*
4) $Q_i = \{P_{1i}, P_{2i}, \dots, P_{ni}\} \in P$;
5) *F* – совокупность правил идентификации и оценки признаков *O*;
6) $A = \{A_1, A_2, \dots, A_m\}$ – знания об алгоритмах и процедурах обработки данных;
7) $K = \{K_1, K_2, \dots, K_k\}$ – знания о средах взаимодействий с пользователем;
8) $M = \{M_1, M_2, \dots, M_l\}$ – знания о методах (моделях, алгоритмах, данных).

Используют при формализации и реализации мониторинга такие «гибкие» инструменты, как онтологии, нейросети, нечеткие системы и ситуационные сценариям мониторинга.

Системность мониторинга безопасности необходима для эффективного мониторинга, его планирования. Без Data Analytics/Mining и аналитической поддержки невозможно решать в реальном режиме задачи мониторинга безопасности.

Сетевые атаки часто бывают многоуровневыми, например, в четырехуровневой форме – уровней:

1) аттестации;
2) сертификации;
3) почтовый;

4) базы клиентов.

Активизируются нейросистемы класса NNBID (Neural Network Based Intrusion Detection) для обнаружения атак на компьютерные системы.

Там, где использовались раньше «жесткие» модели стали использовать «мягкие» модели и навыки или SoftSkills [12]. Они эффективны против гибридных инструментов внедрения в сеть, захвата трафика, активности со злым умыслом (класса SIEM). Одним из гибких и популярных подходов является имитация атак, а также тестирование хаоса в системе.

Проблема мониторинга SOC – многосторонняя и решать ее следует, привлекая различный инструментарий, а также автоматизируя процедуры. Важно поддержать компетенции персонала, минимизировать риск доступа к корпоративным данным, например, базам данных «толстого сервера» при обработке данных «тонким клиентом».

Здесь полезны модели риск-менеджмента информационных систем (сетей) с учетом «белого» (гауссова) шума и его фильтрации.

Предлагаем, например, модель:

$$y = L(x) = (M + \delta)(x),$$

где $x = (x_1, \dots, x_m) \in R^m$ – вектор отслеживаемых при мониторинге факторов, $L(x)$ – оператор прогнозирования с учетом шума, для которого верна гипотеза нормальности распределения.

Тогда «мониторинговая» величина $x(t)$ представима в виде:

$$x = (F + \eta)(x),$$

где F – оператор мониторинга (аудита, оценки) в системе SOC.

В дискретном варианте

$$x_k = x(k),\ k = 0,1, \dots, k$$

запишем рекуррентную модель:

$$x_{k+1} = F_{k+1,k}\,(x_k) + \eta_k.$$

Задаются данные мониторинга:

$$y_k = m_k(x_k) + e_k,$$

где η_k – вектор «шумов» модели, e_k – вектор ошибок мониторинговых наблюдений.

Указанные рекуррентные формулы – типа ансамбля фильтра Калмана, который позволяет сглаживать данные мониторинга даже при небольшой мощности ансамбля.

Направленный мониторинг часто плохо формализуем, а его процедуры – плохо алгоритмизируемы, сами операторы *F* – нелинейного типа. Придется решать и «жесткие», например, классические оптимизационные задачи с ограничениями.

Пример. Пусть $x_k = (x_{k1}, \dots, x_{kn})$, $k = 1, \dots, m$ – вектор погрешностей в узле *k* мониторинга, где:

$$x_{jk}(t+1) = x_{jk}(t) + \Delta a_{jk}(t),$$

$$k = 1, \dots, n;\ j = 1, \dots, m;\ t = 0, \dots, \tau - 1,$$

$\Delta a_{jk}(t)$ – приращение *j*-го параметра мониторинга в *k*-ом узле в момент *t*, а затраты на мониторинговый план $v_{jk}(t)$ равны $s(v_{jk}(t))$. Тогда затраты *S* на мониторинг оцениваются формой вида:

$$S = \sum_{k=1}^{n} \sum_{j=1}^{m} \sum_{t=0}^{\tau-1} s\left(v_{jk}(t)\right).$$

Оптимизационная задача по управлению риск-мониторингом ставится в виде:

$$S \Rightarrow min,$$

$$0 \le v_{jk}(t) \le n_j,$$

$$0 \le x_{jk}(t) \le \varepsilon_j,$$

где n_j – число планов мониторинга, ε_j – допуск точности по параметру *j*.

Чтобы снизить неопределенности (риски) при мониторинге необходимо иметь картину бифуркаций и управляемости процесса. Это также позволит выяснить самоорганизационный потенциал системы.

Бифуркации можно исследовать по модели «реакция-диффузия» вида:

$$\frac{\partial x}{\partial t} = A(u)x + B(x,u)$$

с линейной $A(u)$ и нелинейной $B(x,u)$ составляющими процесса.

При моделировании ситуации безопасности важно прогнозировать как риски, так и закон распределения рисков. Например, по гипотезе равномерного их распределения. Рассмотрим соответствующую модель.

Пример. Пусть $p(t)$ – вероятности временного распределения рисков, $u(t)$ – их плотность, $0 < t < T$, n – отслеживаемые классы рисков. Предлагается модель:

$$u'(t) = \big(A(t) - B(t)u(t)\big)u(t), \qquad u(0) = u_0.$$

Данную модель, которая уточняема с использованием гибких процессов идентификации, можно использовать на практике. Она хорошо адаптируема к ситуационному моделированию.

Выводы

Эффективность Центров автоматизированного мониторинга и управления безопасностью должна соответствовать эволюционным целям системы. Она зависит от выбранных целей, критериев и моделей результативности и эффективности SOC, риск-устойчивости всей экосистемы. Мониторинг проводится как в ручном режиме, так и в автоматизированном или даже автоматическом режиме (на определенном периоде функционирования рассматриваемой системы).

Мониторинг событий, ситуаций безопасности – непрерывный процесс анализа данных по регистрируемым угрозам и риск-уязвимостям цифровой экосистемы. На основе мониторинговых данных проводится анализ

длительности восстановления бизнес-процессов, разрабатывается соответствующая модель и проводится идентификация модели.

В качестве аппарата для моделирования можно использовать, как выше, мультипликативные полуэкспериментальные модели, так и «жесткие» формальные модели на основе марковских процессов, дифференциальных уравнений и др. Но перспективно использовать «мягкие» модели – когнитивные, нейросетевые, мульти-агентные, с применением социальной инженерии и др. В обоих случаях эффективно применение ситуационно-событийного имитационного моделирования.

Заключение

Особенностью современного мониторингового центра является оперативность, отсутствие промежуточных звеньев и адаптивность, реакция на риск-ситуации «на лету», фильтрация шумов и хаос-моделирование ситуаций. Эффективное моделирование риск-ситуаций необходимо для устойчивости и интегрируемости риск-менеджмента и управления инфраструктурой, персоналом и ресурсами.

В цифровой инфраструктуре организации принятие решения на основе ситуационных сценариев требует разработки имитационных моделей и гибких алгоритмов их идентификации с привлечением Big Data, Data Mining, а также эффективных критериев устойчивости инфраструктуры.

Работа может быть развита как в направлении усложнения (углубления) моделей, так и повышения их гибкости, эластичности.

Литература

1. Велигодский С.С., Милославская Н.Г. Унифицированная модель зрелости центров управления сетевой безопасностью информационно-телекоммуникационных сетей. Известия ЮФУ (сер. «Технические науки»). 2023. №3(233). С.157-172. DOI: 10.18522/2311-3103-2023-3-157-172.

2. 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.

3. Глухова Л.В., Казиева Б.В., Казиев В.М., Шерстобитова А.А. Мониторинг и управляемость цифрового бизнеса корпорации. Вестник Волжского ун-та им. В.Н. Татищева. 2022. №1(49). С.14-22. DOI: 10.51965/20767919_2022_2_1_14.

4. Кондаков С.Е., Рудь Н.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 А.С, Марченко М.А. Модель оценки ущерба от инцидентов информационной безопасности. Безопасность информационных технологий. 2021. №2. С.98-106.

6. Гайфулина Д.А., Котенко И.В. Применение методов глубокого обучения в задачах кибербезопасности. Часть 1. Вопросы кибербезопасности. 2020. №3(37). С.76-86. DOI: 10.21681/2311-3456-2020-03-76-86.

7. Гайфулина Д.А., Котенко И.В. Применение методов глубокого обучения в задачах кибербезопасности. Часть 2. Вопросы кибербезопасности. 2020. №4(38). С.11-21. DOI: 10.21681/2311-3456-2020-04-11-21.

8. 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.

9. Золотавин В.С., Нечта И.В. Обзор сетевых атак типа Man-in-the-middle (MITM). В сб: «Обработка информации и математическое моделирование» (Новосибирск, 19–20 апреля 2023 года). 2023. С.188-194. DOI: 10.55648/978-5-91434-085-5-2023-188-194.

10. Herbert S., Why IIoT should make business rethink security. Network Security. 2019. No.7. pp.9-11. DOI: 10.1016/S1353-4858(19)30083-2.

11. Самарский А.А., Гулин А.В. Численные методы. М.: Наука, 1989. 432 с.

12. Максимова Е.А. Когнитивное моделирование деструктивных злоумышленных воздействий на объектах критической информационной инфраструктуры. Труды учебных заведений связи. 2020. №4(6). С.91-103. DOI: 10.31854/1813-324X-2020-6-4-91-103.

References

1. Veligodskij C.C., Miloslavskaya N.G. Izvestiya YuFU (ser. «Texnicheskie nauki»). 2023. №3(233). pp. 157-172. DOI: 10.18522/2311-3103-2023-3-157-172

2. Gos`kova D.A., Massel` A.G. Zhurnal Voprosy` kiberbezopasnosti. 2019. №2. pp. 42-49. DOI: 10.21681/2311-3456-2019-2-42-49.

3. Gluxova L.V., Kazieva B.V., Kaziev V.M., Sherstobitova A.A. Vestnik Volzhskogo un-ta im. V.N. Tatishheva. 2022. №1(49). pp. 14-22. DOI: 10.51965/20767919_2022_2_1_14

4. Kondakov S.E., Rud` N.S. Zhurnal Voprosy` kiberbezopasnosti. 2021. №5. pp. 12-20. DOI: 10.21681/2311-3456-2021-5-12-20.

5. Tany`gin M.O., Budnikova Yu.A., Bulgakova A.S, Marchenko M.A. Bezopasnost` informacionny`x texnologij. 2021. №2. pp. 98-106

6. Gajfulina D.A., Kotenko I.V. Zhurnal Voprosy` kiberbezopasnosti. 2020. №3(37). pp. 76-86. DOI: 10.21681/2311-3456-2020-03-76-86.

7. Gajfulina D.A., Kotenko I.V. Zhurnal Voprosy` kiberbezopasnosti. 2020. №4(38). pp. 11-21. DOI: 10.21681/2311-3456-2020-04-11-21.

8. Vasil`ev V.I., Kirillova A.D., Vul`fin A.M. Zhurnal Voprosy` kiberbezopasnosti. 2021. №2. pp. 2-16. DOI: 10.21681/2311-3456-2021-2-2-16.

9. Zolotavin V.S., Nechta I.V. Obrabotka informacii i matematicheskoe modelirovanie (Novosibirsk, 19–20 aprelya 2023 goda). 2023. pp. 188-194. DOI: 10.55648/978-5-91434-085-5-2023-188-194.

10. Herbert S., Why IIoT should make business rethink security. Network Security. 2019. №.7. pp. 9-11. DOI: 10.1016/S1353-4858(19)30083-2

11. Samarskij A.A., Gulin A.V. Chislenny`e metody. [Numerical methods]. M.: Nauka. 1989. 432 p.

12. Maksimova E.A. Trudy` uchebny`x zavedenij svyazi. 2020. №4(6). pp. 91-103. DOI: 10.31854/1813-324X-2020-6-4-91-103.

Дата поступления: 9.10.2024

Дата публикации: 30.11.2024