МОДЕЛЬ ОЦЕНКИ БЕЗОПАСНОСТИ СЛОЖНОЙ СЕТИ (ЧАСТЬ 1)

Калашников А.О.[1], Бугайский К.А.[2]

Цель статьи: *разработка механизмов оценки действий агентов сложных информационных систем с точки зрения информационной безопасности.*

Метод исследования: *теоретико-игровые модели с использованием методов стохастического моделирования.*

Полученный результат: *дано описание предметной области применения модели, показано, что действия нарушителя и защитника могут рассматриваться с точки зрения получения и дальнейшей эскалации прав доступа на объектах информационной системы. Показано, что модель информационного противоборства защитника и нарушителя может быть представлена тройкой «граф, агент, правила». Дано определение основных терминов и понятий модели. Разработаны базовые принципы функционирования модели. Показана возможность реализации расчетов результатов деятельности агентов и итогов игры в условиях информационной неопределенности. Определен перечень базовых величин модели позволяющих рассчитывать затраты и выигрыши участников игры. Разработаны основные правила расчетов затрат и выигрышей. Определены входные параметры модели, задаваемые при ее инициализации. Показаны роль и место «игры с природой» для вычисления базовых величин модели.*

Научная новизна: *состоит в применении энтропийного подхода к расчету базовых величин, определяющих результаты моделирования отдельных операций и действия агентов в условиях информационной неопределенности.*

Ключевые слова: *модель информационной безопасности, оценка сложных систем, теоретико-игровой подход, информационная неопределенность, игра с природой.*

DOI:10.21681/2311-3456-2022-4-26-38

Введение

Основным трендом в развитии современных информационных систем является переход на широкое использование облачных технологий, включая такие варианты как: «Функция как Сервис» (FaaS) и граничные вычисления (Edge). Также необходимо отметить параллельный бурный рост использования киберфизических устройств в различных областях человеческой деятельности, взаимодействующая совокупность которых, называется обычно «Интернет вещей» (IoT). В целом же можно говорить о том, что современные информационные системы строятся на основе микросервисов и архитектуры «Инфраструктура как Код» (IaC) [1]. Как результат, вопросы информационной безопасности подобных систем приходится рассматривать в рамках сложной сетевой структуры, каждый элемент которой имеет собственные механизмы реализации прав доступа субъектов к объектам. В условиях наличия в составе сложной сети сотен и тысяч таких элементов вопрос оценивания потенциальных путей нарушения прав доступа (и соответственно конфиденциальности, целостности и доступности) представляет собой, как правило, задачу полного перебора.

Одним из способов решения таких задач является имитационное моделирование. В данной работе предложена модель анализа информационной безопасности (далее – ИБ) информационной системы (далее – ИС) как сложной сети. Модель обеспечивает формирование исходных данных для последующего проведения имитационных экспериментов на основе многократного выполнения различных последовательностей шагов взаимоувязанных процессов атаки и защиты. Имитация выполнения последовательности

1 Калашников Андрей Олегович, доктор технических наук, главный научный сотрудник лаборатории «Сложных сетей» ФГБУН Институт проблем управления им. В.А. Трапезникова РАН, г. Москва, Россия. E-mail: aokalash@ipu.ru

2 Бугайский Константин Алексеевич, младший научный сотрудник лаборатории «Сложных сетей» ФГБУН Институт проблем управления им. В.А. Трапезникова РАН, г. Москва, Россия. E-mail: kabuga@ipu.ru

шагов нацелена на оценку соотношений затраты-приобретения ресурсов и динамику их изменений в процессах атаки и защиты. Формируемые последовательности шагов используемых при имитации процессов атаки и защиты обеспечивают необходимую вариативность моделирования указанных процессов.

Описание предметной области

Определим ИС как набор элементов и связей между ними. Для ИС набор элементов должен представлять собой различные комбинации документов (под которыми будем понимать документацию, информационные ресурсы, базы данных и пр.), программных и аппаратных средств, а также персонал (пользователей). С точки зрения ИБ целесообразно документы (в смысле, определенном выше), аппаратные и программные средства рассматривать как объекты, а персонал — как субъекты модели ИС. Защите подлежит информация, обрабатываемая в ИС — документы в терминах модели. Но, необходимо отметить, что:

- информация (документы) ИС может существовать только на физических носителях;
- обработка информации в ИС может осуществляться только с помощью программных средств — процессов (активных или работающих) в терминах модели.

Таким образом, ИС может быть представлена в виде сложного графа (сети), состоящего из узлов, каждый из которых включает в себя определенный наборов документов и процессов [2]. При этом следует учесть, что:

- работа процессов узлов определяется специальными документами — *конфигурациями*, являющимися неотъемлемой частью узлов и входящих в сферу ИБ с точки зрения защиты таких документов;
- защита информации в ИС может быть обеспечена только путем управления правами доступа субъектов к объектам.
- Особенность современных программных (прежде всего) и аппаратных средств заключается в том, что в рамках одного узла (элемента) ИС все права доступа (прежде всего — модификация, удаление и создание документов и процессов) можно разделить на два типа:
- права пользователя в отношении ограниченного набора процессов и документов;
- права супер-пользователя (администратора, системы) в отношении всех процессов и документов узла.

При этом, как правило, пользователю доступна для чтения или запуска значительно большая часть документов и процессов, чем для изменения. В модели учтено, что наличие прав пользователя на узле дает возможность собирать значительные объемы информации о конфигурации как узла, так и ИС в целом. Современные тенденции и принципы построения ИС требуют, чтобы модель обеспечивала:

- учет виртуализации, которую можно рассматривать как вложенность узлов;
- учет нескольких уровней управления — на каждом из уровней вложенности как минимум.

В качестве иллюстрации можно привести случай аренды виртуальных машин у провайдера облачной инфраструктуры. Следует учесть, что нарушение прав доступа на одном из уровней вложенности означает получение прав собственности над узлами на нижележащих уровнях. Таким образом, ИС — как сложная система — должна быть представлена в виде графа, учитывающего вложенности узлов. Этого можно достичь, если рассматривать различные типы связей узлов на графе:

- обмен данными в рамках вложенности в контейнерах;
- обмен данными в рамках управления узлами;
- обмен данными между узлами.

При этом необходимо учитывать, что:

- первые два обмена могут быть представлены отношением «родитель – потомок»;
- все обмены имеют двухсторонний характер;
- один узел может иметь несколько связей и как родитель и как потомок.

Процессы ИБ в ИС могут быть представлены как действия защитника по управлению правами пользователя и как действия нарушителя по нарушению (присвоению и/или эскалации) этих прав [3 - 11]. Действия нарушителя приводят к получению прав на уровне легитимного пользователя или супер-пользователя узла. Без потери общности в рамках модели нарушитель и защитник могут рассматриваться как активные сущности – агенты, а остальные пользователи ИС как пассивные сущности – носители тех или иных прав доступа к документам и процессам. В силу свойства активность/пассивность в модели рассматриваются только действия нарушителя и защитника. В самом общем виде смысл деятельности нарушителя заключается в нанесении ущерба ИС в том или ином виде, а защитника – в предотвращении такого ущерба. Но поскольку понятие полного ущерба предполагает включение в модель бизнес-процессов обслуживаемых

данной ИС, рассмотрение всех характеристик и видов ущерба приведет к значительному усложнению модели. Поэтому целесообразно:

- принять в качестве ущерба нарушение конфиденциальности, целостности и доступности (далее – КЦД) информации в ИС;
- рассматривать глобальные цели защитника и нарушителя, а также способы их достижения.

Тогда деятельность нарушителя и защитника может рассматриваться как антагонистическая игра, а в качестве стратегий игроков – распределение некоторого ресурса. Без потери общности процессы ИБ в ИС можно рассматривать в виде тройки «нарушитель, защитник, атака».

Описание нарушителя

Для целей моделирования рассматриваются следующие глобальные цели деструктивных действий нарушителя:

а) получение несанкционированного доступа к информации (далее – НСД);

б) нарушение штатного режима работы ИС.

Получение НСД предполагает, что нарушитель заинтересован в получении как можно более полного доступа к хранящимся в системе данным. Нарушитель может быть заинтересован в получении некоторой конкретной информации, однако чаще при таких атаках нарушителя интересует как можно более полный сбор всех доступных сведений. Такой нарушитель, как правило, заинтересован в долговременном использовании результатов атаки. Это означает, что чем дольше его действия остаются незамеченными, тем больший выигрыш он получает от осуществленной атаки. Цель нарушения штатной работы системы можно представить как стремление к нарушению КЦД. Нарушение целостности информации означает, что нарушитель модифицирует данные или процесс таким образом, чтобы повлиять на работу системы. Нарушение доступности информации влечет как правило временную остановку деятельности узлов ИС. Что может быть организовано, например, с помощью атаки на отказ в обслуживании на каналы доступа к ИС.

В самом общем случае следует положить, что получение НСД и разрушение инфраструктуры ИС предполагает также получение прав администратора в самой ИС или на различных уровнях вложенности ее инфраструктуры. В рамках модели будем считать, что действия нарушителя определяются следующими мотивами:

- обеспечение максимальной скрытности своих действий;
- распространение своего влияния на максимальное число узлов ИС;
- получение максимально возможного контроля над процессами как на отдельных узлах, так и в ИС в целом.

С одной стороны, определение целей и мотивов нарушителя выходят за пределы модели и может быть сформулировано только на основании экспертной оценки. С другой — целесообразно рассматривать комбинации перечисленных мотивов как стратегии поведения нарушителя, базирующиеся на получении прав доступа. Реальный нарушитель может комбинировать данные мотивы в процессе осуществления атаки, направленной на достижение некой глобальной цели. Достижение которой должно рассматриваться как последовательное – через доступные связи – перемещение нарушителя по узлам ИС с целью установления контроля над как можно большим числом узлов или как целенаправленное движение к конкретному узлу. При этом целесообразно учитывать расположение нарушителя относительно ИС:

- внутри ИС, если нарушитель обладает правами пользователя или если имеет доступ к инфраструктуре ИС (особенно актуально для географически распределенных облачных систем).
- извне ИС, если нарушитель может осуществить подключение к системе с использованием или нет данных авторизации или, когда злоумышленник получает контроль над внешними ресурсами, используемыми ИС (ее пользователями).

Внешнее расположение нарушителя относительно ИС (на отдельном узле вне графа ИС) предполагает выделение на графе ИС определенных узлов и внесение дополнительных связей этих узлов с внешним узлом нарушителя.

Описание защитника

Для целей моделирования будем полагать, что цели защитника противоположны целям нарушителя и представляют собой действия по недопущению НСД и сохранению/восстановлению КЦД и работоспособности системы. В качестве мотивов, определяющих действия защитника, можно указать следующие:

а) мониторинг инфраструктуры;

б) противодействие нарушителю.

Мониторинг инфраструктуры предполагает не только сокращение времени на обнаружение деструктивных действий нарушителя, но и получение информации, позволяющей:

- определить цель перемещений нарушителя по графу ИС;

— оценить уровень его осведомленности о состоянии инфраструктуры;
— осуществить отбор наиболее опасного сценария развития атаки.

Противодействие нарушителю предусматривает не только достижение целей защиты, но и выполнение действий по блокированию атаки, включающих:

— увеличение затрат нарушителя на выполнение дальнейших действий, в том числе за счет повышения защищенности узлов на основе выявленных действий нарушителя;
— создание ложных целей и сокращение доступных нарушителю узлов и связей между ними если это допускают бизнес-процессы ИС.

Возможные комбинации мотивов действий защитника образуют его стратегии действий по защите информации в ИС. Мероприятия по противодействию нарушителю также формализуются в виде «перемещения» защитника по графу. Но, в отличие от нарушителя, защитник, как правило, действует на известной ему топологии графа. С учётом этого обстоятельства, защитнику не требуется совершать последовательных переходов по рёбрам графа, т. е. защитник может занимать в любой момент любую вершину графа.

Отметим, что построение современных ИС имеет выраженную тенденцию к гибридизации инфраструктуры. Например, сочетание частного и гибридного облаков, аренда ресурсов у различных провайдеров услуг, различные комбинации «классических» серверов и систем (типа АСУ ТП) с различными вариантами виртуализации. Все это говорит о необходимости введения в модель нескольких защитников с определенными зонами ответственности. Кроме того, в пользу такого решения выступают положения руководящих документов об организации ИБ в ИС. Тогда можно разделить защитников на типы по преимущественной реализации мотивов защиты:

— администраторы ИБ (АИБ) - преимущественно занимающиеся анализом целей и сценариев поведения нарушителя на основе результатов мониторинга;
— администраторы ИТ (АИТ) - осуществляющие непосредственное противодействие атаке на объектах (элементах) ИС в зоне своей ответственности или компетентности.

При этом АИБ могут осуществлять непосредственное администрирование средств защиты информации (далее – СЗИ), включенные в качестве отдельных узлов в граф, описывающий ИС. Что, в частности, позволяет моделировать усложнение условий для развития атаки. Модель должна обеспечивать возможность анализа как на уровне отдельного защитника, так и на уровне группы защитников, действующих самостоятельно. Вопросы кооперативного действия защитников на уровнях обмена информации, согласования действий, выбора цели защиты и т. п. в настоящей статье не рассматриваются.

Описание атак

Поскольку в основе модели лежит теоретико-игровой подход, то атака рассматривается как противоборство нарушителя и защитника, выражающееся в поочередном выполнении тех или иных последовательных действий. Реализация стратегий по достижению глобальных целей для нарушителя и защитника могут быть описаны обобщенными алгоритмами.

Обобщённый алгоритм поведения нарушителя может быть описан в виде трех стадий:

1. Вторжение в систему – происходит первичное инфицирование ИС, как правило, выражающееся в установлении нарушителем контроля над одним из объектов (элементов) ИС В рамках модели такой объект – точка вторжения – может задаваться целевым или случайным образом.

2. Развитие атаки – на этой стадии нарушитель последовательно перемещается по объектам (графу) ИС и пытается установить над ними необходимый контроль чтобы определить объекты, соответствующие целевым установкам.

3. Финальная стадия атаки, при которой происходит собственно реализация целей и мотивов атакующего (несанкционированный доступ к объектам, выведение объектов из строя и пр.).

Положим, что реализация алгоритма нарушителя будет проявляться в получении им определенных прав на узле, допускающих изменение состояния документов и процессов из его состава.

Обобщённый алгоритм поведения защитника также может быть описан в виде трех стадий:

1. Выполнение определенных действий на узлах, повышающих уровень обнаружения атак.

2. Поиск вторжения в систему. Целенаправленный (последовательный) или случайный обход узлов с целью обнаружения изменений текущих прав субъектов на объекты относительно легитимных.

3. Противодействие атаке, предполагающее определение пораженных узлов и выполнение тех или иных действий по повышению уровней обнаружения атак или защищенности на смежных узлах.

DOI:10.21681/2311-3456-2022-4-26-38

Вопросы восстановления штатных прав доступа на узлах, а также нарушения каналов управления со стороны нарушителя являются предметом отдельного исследования, поскольку без принятия дополнительных мер это вызывает зацикливание в работе модели, связанное с нарушением/восстановлением прав доступа на одном и том же узле на последовательных ходах нарушителя и защитника.

Необходимо отметить следующую особенность реализации алгоритмов нарушителя и защитника. В каждый конкретный момент времени нарушитель и защитник могут выполнять те или иные действия только с определенным узлом. Что позволяет говорить о реализации локальных целей на этом узле. Для упрощения модели будем считать тождественными понятия «локальная цель» и «действие агента».

Действия нарушителя

ДН1 – получение прав неавторизованного пользователя и выполнение доступных действий (например, формирования пакетов для их прохождения через прокси или балансировщик);

ДН2 – получение прав текущего пользователя без деструктивного воздействия (например, кража или получение установочных данных из других источников и их использование);

ДН3 – получение прав текущего пользователя в результате деструктивного воздействия;

ДН4 – получение системных прав (супер-пользователя) без деструктивного воздействия;

ДН5 – получение системных прав (супер-пользователя) в результате деструктивного воздействия.

Следует отметить, что приведенный перечень действий не является исчерпывающим или обязательным и может расширяться или видоизменяться. Результаты выполнения действий нарушителем отображаются в изменении статуса узла.

Действия защитника

ДЗ1 – контрольная проверка (опрос) состояния всех точек мониторинга;

ДЗ2 – изменение узла для усиления функций мониторинга действий нарушителя (создание новой точки мониторинга);

ДЗ3 – изменение узла для усиления защитных свойств (включая изменение настроек и режимов работы);

ДЗ4 – отключение узла (инцидентного ребра) от смежного узла, захваченного нарушителем;

ДЗ5 – изменение стоимости узла с целью создания узла-приманки за счет изменений в процессах и документах.

Для упрощения модели будем полагать, что защитник может оценивать действия нарушителя только по результатам захвата узлов, являющихся точками мониторинга и усиленной защиты. Соответственно, нарушитель не имеет информации о наличии и расположении таких узлов.

Следует отметить, что приведенный перечень действий также не является исчерпывающим или обязательным и может расширяться или видоизменяться.

Положения данного раздела позволяют рассматривать деятельность нарушителя и защитника как противоборство, «полем» которого выступает ИС. Противоборство заключается в попытках нарушить КЦД узлов ИС со стороны нарушителя и противодействие этим попыткам со стороны защитника. Таким образом, в основу модели может быть положен теоретико-игровой подход. При этом ИС может быть представлена в виде графа, действия нарушителя и защитника – как перемещение по ребрам графа и выполнение определенных действий над элементами ИС – вершинами или узлами графа [3, 12 - 14].

Основания модели

На основании [15 - 17] в рамках модели сделаем следующие допущения.

Д1. Перемещение агентов (здесь и далее – атакующий или защитник) по узлам графа, подчинено достижению некоторой глобальной цели. В каждый конкретный момент времени агент выполняет те или иные операции с определенным узлом ИС. При этом каждому узлу графа может быть поставлена в соответствие определенная локальная цель, которая может быть достигнута в результате выполнения соответствующего набора действий (шагов). То есть, действия агентов могут быть представлены в виде последовательности шагов:

- выбор атакуемого в данный момент времени объекта;
- формирование локальной цели для этого объекта;
- выполнение необходимого набора операций по достижению локальной цели.

Д2. Возможности агентов по реализации тех или иных действий на узле, касающихся КЦД, определяются уровнем полномочий, получаемых в ходе выполнения операций. Получаемые агентом уровни полномочий на узлах являются отображением:

— результата предпринятых агентом действий;
— потенциальных возможностей агента по дальнейшим действиям.

Д3. В модели целесообразно рассматривать только поведение агентов в процессе реализации атаки, поскольку подготовительные действия атакующего проходят вне графа ИС – пространства игры (модели), а действия защитника по защите информации формируют граф ИС – пространство игры.

Д4. Каждый узел графа ИС имеет определенную ценность для агентов как с точки зрения КЦД, так и с точки зрения развития атаки. При этом ценность одного и того же узла для разных агентов может быть разной.

Д5. Атакующий и защитник на одном узле не могут иметь одинаковые права, но допустим случай, когда защитник имеет права супер-пользователя, а атакующий – пользователя.

Д6. Действия агентов по реализации атаки и противодействию ей рассматриваются исключительно с точки зрения получения прав пользователя на узле. Все действия агентов, направленные на изменение КЦД узла можно рассматривать как одно «универсальное» действие при наличии необходимых прав. То есть важен сам факт получения прав пользователя (а тем более – супер-пользователя) на узле.

Исходя из сказанного выше, можно дать следующие определения.

Захватом узла называется факт получения агентом прав пользователя на узле.

Состоянием игры (позицией) называется вектор, описывающий распределение прав агентов по узлам.

Ценностью узла называется некоторая количественная характеристика (например, целое или действительное число) отражающая роль узла в ИС и качественные характеристики обрабатываемой информации. Ценность узла может рассматриваться как показатель количества и качества потенциально доступной агенту информации (в случае захвата узла).

Потенциалом агента называется количественная характеристика, отражающая его возможности по перемещению на графе ИС (число захваченных узлов и доступных связей) и имеющиеся (полученные) права на захваченных узлах за счет способности выбрать и успешно реализовать оптимальный набор действий.

Статусом узла называется вектор, описывающий текущее распределение прав доступа агентов на узле.

Д7. В рамках теоретико-игрового описания целесообразно рассматривать действия агента по получению прав на узле как приложение определенных усилий, которые должны иметь количественную оценку. Усилия по захвату узла могут быть многократно меньше ценности узла.

Д8. Достижение цели считается реализованным только в случае успешного выполнения всех операций соответствующего набора, что отображается в изменении статуса узла.

Понятие успеха может различаться для разных операций, но можно выделить две составные части понятия. Для успешного выполнения операции необходимо наличие:

— условий как набора необходимых объективных предпосылок для выполнения операции;
— возможностей как набора достаточных инструментов для выполнения операции.

Отсюда вытекает понятие квалификации агента.

Квалификация агента — его способность подобрать и использовать доступные инструменты адекватные условиям для выполнения операции.

Д9. Любая операция увеличивает знания агента об объекте взаимодействия – от узла до сложной сети в целом. Соответственно, можно дать следующие определения:

Ценность операции – это полученная в результате ее выполнения ранее не известной информации.

Информированность агента – это совокупность его знаний как об отдельных узлах графа ИС, так и о графе в целом. Информированность является аддитивной функцией, зависящей от выполненных операций и захваченных узлов.

Таким образом, в основе описания деятельности агентов лежит кортеж:

$$\langle \text{ценность узла, усилия агента, потенциал агента, ценность операции, информированность агента} \rangle \quad (1)$$

Для дальнейшего синтеза модели необходимо определить единую меру для элементов кортежа.

Основываясь на [16], будем предполагать, что в общем случае агент действует в условиях неопределенности. Если учесть, что полную информацию об атакуемом узле агент получит только после получения соответствующих прав на нем, то можно считать, что деятельность агента направлена на снижение степени неопределенности или повышение своей информированности в процессе достижения главной цели. Ограниченность информации до выполнения действий, неопределенность результатов выполняемых действий и неполнота (ограниченность) получаемой по этим результатам информации дают основания рассматривать достижение агентом локальной цели как «игру с природой».

Таким образом, основная деятельность агента представляет собой выполнение операций для уменьшения неопределенности при достижении глобальной или локальной цели. Тогда деятельность агента можно рассматривать как реализацию двух событий – получение и оценивание информации о состоянии узла в результате успешного выполнения определенного действия. События получения информации и успешности необходимых для этого действий взаимосвязаны и взаимообусловлены.

Пусть имеем событие A – получение и оценивание информации в результате наступления события B – успешной реализации действия. Используя энтропийный подход запишем:

$$H(A|B) = H(A) - H(B) + H(B \mid A) \quad (2)$$

Выражение (2) показывает, насколько уменьшится неопределенность агента за счет получения информации в результате реализации действия. Дадим трактовку членам выражения с точки зрения описанной ранее предметной области:

- $H(A|B)$ – прирост информированности агента в случае успешности выполнения действий (операций) на узле (против узла);
- $H(A)$ – ценность узла (операции) с точки зрения агента – максимально возможное уменьшение неопределенности, возникающее при получении наибольших прав доступа на узле;
- $H(B)$ – уменьшение неопределенности, вызванное способностью агента выбрать и успешно реализовать оптимальное действие или потенциал агента;
- $H(B \mid A)$ – успешность выполнения действий в зависимости от имеющейся информации или оценка усилий агента.

Последний член выражения (2) нуждается в дополнительном обсуждении. Он описывает неопределенность события B при условии наступления события A. Но в рамках проблемной области событие A нужно трактовать как наличие информации предшествующей событию B. Тогда, выражение (2) можно переписать как:

$$H(A_n|B_n) = H(A_n) - H(B_n) + H(B_n \mid A_{n-1}),$$

где n – порядковый номер шага агента при реализации локальной или глобальной цели.

Соответственно можно говорить о рекуррентной функции, описывающей деятельность агента по реализации его стратегии в течение всего времени выполнения атаки.

В нашем случае вид функции $H(*)$ не имеет принципиального значения. Гораздо важнее, что выражение (2) позволяет говорить о наличии единой безразмерной шкалы $[0,1]$ оценивания всех основных параметров, описывающих деятельность агента. Тогда в соответствии с ресурсной моделью атаки [6] можно говорить о представлении неопределенности как некоторого ресурса Θ с помощью функции отображения $f^*: H(*) \to \Theta$. Но тогда необходимо говорить и о наличии функции отображения усилий Ω агента по уменьшению неопределенности $H(*)$: $g^*: \Omega \to H(*)$. Что дает возможность при рассмотрении деятельности агента говорить о функции $u^* = g^* \circ f^*$ – композиции двух предыдущих функций.

Мерой неопределенности является энтропия, позволяющая в общем случае оценить количество информации, получаемой агентом в случае выполнения тех или иных действий. Рассмотрим с этих позиций еще раз кортеж (1), описывающий деятельность агента с учетом трактовок выражения (2).

Ценность узла и ценность операции. Чем выше ценность узла или операции, тем больше информации получает агент. Что можно трактовать как приращение ресурса. Соответственно, с повышением ценности должно увеличиваться приращение ресурса.

Усилия агента. Зависимость успеха выполнения действий от имеющейся информации позволяет рассматривать усилия именно как ресурс, потраченный на сбор и обработку необходимой информации. Тогда чем больше информации имеет агент перед выполнением действий, тем больше ресурса он израсходовал.

Потенциал агента характеризует его возможности по перемещению на графе ИС (число захваченных узлов и доступных связей), вытекающие из имеющихся (полученных) прав на захваченных узлах. Представляется очевидным, что чем выше права агента на узле, тем больше он имеет информации и тем выше его потенциал.

Информированность агента. Согласно выражению (2), информированность агента является интегральной характеристикой. Соответственно, чем ценнее узел и чем успешнее выполнены действия в отношении его (2), тем больше информации и ресурса получает агент.

В соответствии со сказанным выше в рамках модели будем считать, что выражение для ресурса имеет вид:

$$\Theta = au^* + b \quad (3),$$

где:

a – коэффициент масштаба, задающий число единиц ресурса размером ε, размещаемых на шкале [0, 1];

b – коэффициент сдвига, задающий минимально воз-

можное число единиц ресурса в зависимости от рассматриваемой характеристики деятельности агента.

Оценка базовых величин модели

Исходя из изложенного выше можно выделить некоторые переменные модели, которые являются атомарными (неделимыми) и определяют все последующие расчеты.

1. *Ценность узла*. Ценность или стоимость узла определяется количественной – степень вершины графа (узла) и качественной – функциональность – характеристиками. Обе характеристики будем рассматривать, как источники роста потенциала агента. Функциональная характеристика узла w_v^f может определяться общепринятым способом для качественных характеристик – по шкале Харрингтона от значения «очень низкий» до значения «очень высокий». Это позволяет абстрагироваться от конкретных особенностей внутренней структуры узла, но позволяет оценить его роль и место в ИС. Степень вершины узла является непосредственным отображением его привлекательности для атакующего или важности для защитника. Кроме того, степень вершины любого узла дает дополнительную информацию о структуре графа и определяет возможности агента по дальнейшему продвижению по графу. Каждое инцидентное ребро вершины в наиболее общем виде может быть охарактеризовано вероятностью успешной реализации действий агента. Положим, что эти вероятности одинаковы для всех ребер независимо от типа агента. При этом следует считать, что для каждого из инцидентных ребер действия агента представляют собой независимые и несовместные события. То есть, можно выразить количественную характеристику ценности узла w_v^e с информационной точки зрения как: $w_v^e = \ln\sigma$, где σ – число инцидентных ребер узла v. Тогда мы можем получить верхнюю оценку стоимости узла $w_v^+ = w_v^f + w_v^e$. Верхняя оценка w_v^+ соответствует успешной реализации действий направленных на получение максимальных прав доступа на узле. Что соответствует действиям агента типа Д5 для атакующего или защитника. Определим нижнюю оценку стоимости узла. Как следует из описания деятельности агента и описания предметной области, наиболее распространенными для атакующего и защитника будут действия типа Д1. С одной стороны, такие действия практически не зависят от функциональной ценности узла w_v^f, но, с другой стороны, для выполнения агентом действий типа Д1, узел должен содержать в себе некий базовый функционал. Эмпирически установим, базовый функционал узла $w_v^b = 0{,}1 w_v^f$. Тогда нижняя оценка ценности узла $w_v^- = w_v^b + w_v^e$. Наличие нижней и верхней оценок стоимости узла и их соотношение с действиями агента дают основание рассматривать стоимость узла, как интервал $\left[w_v^b, w_v^f\right]$ на единой шкале, смещенный на величину w_v^e относительно начальной точки отсчета шкалы. Такой подход позволяет оценить выигрыш агента в результате выполнения тех или иных действий на узле. Исходя из выражения (3) можно записать, что стоимость узла равна:

$$w_v = \alpha w_v^f + w_v^e \qquad (4),$$

где α – масштабный коэффициент. Который, исходя из традиционного представления вероятностей, целесообразно принять равным 100.

2. *Выигрыш агента*. Выигрыш агента является необходимой при теоретико-игровом подходе интегральной величиной, характеризующей успешность его действий. Выигрыш агента увеличивает его потенциал или снижает неопределенность в результате успешной реализации последовательности операций по достижению локальной цели на узле. Тогда вероятность успешной реализации отдельной операции можно рассматривать как событие, а действие как последовательность событий с определенными вероятностями p_i. Каждая операция дает (независимо от успешности) агенту некоторую информацию и чем выше вероятности успеха отдельных операций, тем больше снижается неопределенность агента. Пусть действие состоит из τ операций. Тогда общая неопределенность относительно узла будет максимальна при условии равной вероятности для всех операций $H^+ = \ln\tau$. Итоговая неопределенность после выполнения всех операций будет определяться (по Шеннону), как $H^\tau = \sum_{i=1} p_i \ln p_i$. Соответственно выигрыш агента как снижение неопределенности равен $H^- = H^+ - H^\tau$. В соответствии с выражением (2) можно оценивать выигрыш агента его по той же шкале, что и стоимость узла. Для перевода величины H^- в единицы ресурса используем приведенные ранее соотношения между действиями агента (атакующего и защитника) Д1 и Д5, успешная реализация которых соответствуют – в случае представления стоимости узла как шкалы – минимальному и максимальному значениям этой шкалы. Тогда выигрыш агента в результате успешной реализации действия может быть представлен в виде:

$$b_v = H^- * w_v \qquad (4).$$

Таблица 1

Значения функции усилий агента

ρ,μ,θ	0 0 0	1 0 0	0 1 0	1 1 0	0 0 1	1 0 1	0 1 1	1 1 1
γ	0,69	1,1	1,1	1,39	0	0,41	0,41	0,69

3. *Затраты агента*. Затраты агента определяются на конкретном узле для каждого выполняемого действия количеством входящих в его состав операций и их стоимостью. Стоимость отдельной операции определяется прежде всего ее сложностью ρ, но также зависит от условий ее применения – состояния узла μ. С другой стороны, стоимость операции имеет субъективную характеристику – зависимость от квалификации агента θ. Поэтому стоимость операции будем рассматривать обобщенно – в виде функции усилий агента $\gamma = f(\rho,\mu,\theta)$. Сложность операции и квалификацию агента в рамках модели целесообразно определять по шкале качественных оценок Харрингтона, то есть $\rho \in [0,1]$ и $\theta \in [0,1]$. Состояние узла $\mu \in [0,1]$ имеет различные трактовки для операций защитника и атакующего, поэтому целесообразно различать эти величины: $\mu = \{\mu\ ,\ \mu\}$. Для атакующего состояние узла μ можно рассматривать как некий уровень защищенности узла, который необходимо преодолеть для успешного завершения операции. Для защитника состояние узла μ является характеристикой, описывающей свойства узла прежде всего с точки зрения выявления действий атакующего (мониторинга). Отметим, что для атакующего γ должна монотонно и непрерывно расти с ростом ρ и μ, но убывать с ростом θ. Для защитника ситуация аналогична, поскольку увеличение показателей мониторинга влечет увеличение затрат на их обработку. С учетом требований непрерывности и монотонности по каждой переменной целесообразно определить функцию усилий агента как $\gamma = \ln\left(\frac{\rho+\mu}{\theta}\right) = \ln(\rho+\mu) - 1$. С учетом особенностей логарифмической функции проведем нормировку ее переменных следующим образом: $\gamma = \ln((1+\rho)+(1+\mu)) - \ln(1+\theta)$. Тогда получаем область определения функции усилий агента от 1 до 4 и область значений – от 0 до 1,4. В таблице 1 приведены значения функции γ для различных сочетаний ρ, μ и θ в их предельных значениях 0 и 1.

Усилия агента отсутствуют при его максимальной квалификации и равенству 0 параметров сложности операции и состояния узла. Напротив, усилия агента максимальны при равенстве 0 его квалификации, но наибольших значениях сложности операции и состояния узла. Такое распределение значений соответствует реальным обстоятельствам деятельности агента. Приведем граничные значения функции для аргументов равных 0,1 и 0,9. Тогда получаем $\gamma = 1,24$ при наибольших усилиях агента $\rho = \mu = 0,9$ и $\theta = 0,1$, а при наименьших, когда $\rho = \mu = 0,1$ и $\theta = 0,9$, соответственно получаем $\gamma = 0,24$,. Следует обратить внимание на значения функции при равных аргументах. С точки зрения энтропийного подхода это можно рассматривать как максимум энтропии для оценки затрачиваемых агентом усилий на выполнение операции. Согласно формуле частотной энтропии $H^i = \ln\frac{1}{p_i}$ можно записать $\gamma = \ln\frac{1}{p_i}$ для отдельной операции и тогда $p_i = 1/e^{\gamma}$ можно трактовать как пороговое значение, которое необходимо преодолеть для успешного выполнения операции. Для приведенных ранее граничных значений функции усилий агента получаются следующие пороговые значения для вероятности успешного выполнения операции: $\gamma = 0,24,\ p_i = 0,79$ и $\gamma = 1,24,\ p_i = 0,29$. Таким образом, можно записать, что пороговое значение вероятности успешной реализации операции не превышение которого требует повторного выполнения данной операции равно:

$$\delta = 1/e^{\gamma} \qquad (6).$$

В соответствии с (2) и (3) для выражения затрат агента в единицах ресурса необходимо определить масштабный коэффициент. Агент может определить ценность узла только в результате выполнения определенных действий, которые – в силу их определения – могут быть представлены как доли на отрезке $[w_v^b, w_v^f]$. Тогда можно записать πw_v^f, где $\pi \in [0,1]$ – масштабный коэффициент, показывающий долю отдельного действия агента на отрезке $[w_v^b, w_v^f]$. Соответственно, усилия агента по выполнению конкретной операции могут быть представлены как доля от максимального усилия по выполнению операций $\sigma_i = \gamma_i / \gamma_{max}$, где $\gamma_{max} = 1,24$. Поскольку каждое

действие представляет из себя набор операций, то конечные затраты агента на реализацию того или иного действия c_v являются аддитивной функцией усилий агента по выполнению операций:

$$c_v = \pi w_v^f \sum_{i=1}^{\tau} \sigma_i \quad (7).$$

Выражение (7) дает нижнюю оценку, то есть минимально необходимые затраты агента на выполнение операций. Отметим, что ценностные (и ресурсные) характеристики деятельности агента необходимо будут различаться для атакующего и защитника до момента получения системных прав доступа на узле, что соответствует $\pi = 1$.

4. *Определение успешности выполнения операций является необходимым для расчетов затрат и выигрышей агента*. В основу определения успешности положены следующие предположения:

а) для успешного осуществления операции необходимо наличие определенных условий в конфигурации и режимах функционирования объекта;

б) для успешного осуществления операции необходимо наличие определенных возможностей (инструментов) у агента;

в) успешность выполнения операции зависит от способности агента находить и использовать условия и возможности, то есть от квалификации агента.

Полный учет всех условий и возможностей является практически невыполнимой задачей (например, наличие уязвимостей нулевого дня или разработка индивидуальных эксплойтов для конкретных атак). Однако методом Монте-Карло возможно провести моделирование вероятности наличия условий и возможностей как двух случайных величин, которые в рамках противоборства можно рассматривать как независимые. Для получения значений двух случайных величин β^1 и β^2 необходимо использовать два независимых генератора случайных чисел таким образом, чтобы вырабатываемые значения образовывали пары β_i^1 и β_i^2. Формирование пар обеспечивает моделирование необходимого соответствия условия и возможностей. То есть каждая генерируемая пара представляет собой возможный вариант соответствия вероятностей наличия условий и возможностей для отдельного узла. Положим, что способности агента по использованию условий и возможностей, представленных каждой парой β_i^1 и β_i^2, определяется его квалификацией. Тогда, определив математическое ожидание m^1, m^2 для каждой из сгенерированных случайных величин β_i^1 и β_i^2, мы может определить доверительный интервал, при попадании в который будем считать, что условия или возможности могут быть использованы агентом. Доверительный интервал сформируем как $\varepsilon^* = m^* \mp (\theta / 2)$. Тогда проведем преобразование случайных величин β_i^1 и β_i^2 по следующему правилу:

$$\beta'^* = \begin{cases} 1, \beta^* \in \varepsilon^* \\ 0, \beta^* \notin \varepsilon^* \end{cases}$$

Это дает возможность сформировать новую случайную величину y, отражающую состояние пар β_i^1 и β_i^2 для всех N значений:

$$y_i = \begin{cases} 1, \forall i i = [1, N] \exists i \left(\beta_i'^1 = 1 \wedge \beta_i'^2 = 1\right) \\ 0, \forall i i = [1, N] \exists i \left(\beta_i'^1 = 0 \vee \beta_i'^2 = 0\right) \end{cases}$$

Полученные таким образом значения y_i случайной величины y показывают для каких из N сгенерированных пар β_i^1 и β_i^2, $i = [1, N]$, агент может одновременно использовать имеющиеся для данного узла возможности и условия, то есть успешно выполнить операцию, определяемую данными возможностями и условиями. Тогда можно определить величину:

$$p = \frac{1}{N} \sum_{i=1}^{N} y_i \quad (8),$$

как вероятность успешного выполнения операции. В соответствии с (6) можно записать правило $P \le \delta$, определяющее необходимость повторного выполнения операции агентом.

Завершая описание базовых величин модели, укажем с учетом (5–8) правила расчета затрат и выигрыша агента:

$$C^a = \sum_{v=1}^{|V|} c_v, \forall p \vee \forall \delta \quad (9),$$

$$B^a = \sum_{v=1}^{|V|} b_v, \exists (p > \delta) \quad (10),$$

Заключение

В первой части статьи на основании описания предметной области в классических терминах ИБ – нарушитель, защитник, атака – предложено рассматривать вопросы защиты информации, как противоборство агентов в рамках теоретико-игровой модели. Реализация противоборства может быть представлена как выполнение агентами определенной очередности операций по определенным правилам получения и использования прав пользователя и системных прав

на узле. Таким образом модель противоборства может быть представлена тройкой «граф, агент, правила» и описана, как перемещения агентов по графу на основе заданных правил. Показано, что все операции по достижению локальных и глобальной цели выполняются агентом в условиях неопределенности. Приведены и определены базовые величины модели, позволяющие рассчитывать затраты и выигрыш агентов на основе безразмерных единиц ресурса. Расчеты базируются на стохастическом моделировании методом Монте-Карло «игры с природой». Для проведения расчетов задаются входные параметры модели, в качестве которых – кроме собственно графа ИС – используются ценность узла, сложность операции, квалификация агента, состояние узла. Все входные параметры модели должны задаваться на этапе ее инициализации. Полное описание модели на основе тройки «граф, агент, правила» будет сделано во второй части статьи.

Литература

1. Калашников А.О. Инфраструктура как код: формируется новая реальность информационной безопасности / А.О. Калашников, К.А. Бугайский // Информация и безопасность. 2019. Т. 22. № 4. С. 495-506.
2. Лаврова Д. С. Моделирование сетевой инфраструктуры сложных объектов для решения задачи противодействия кибератакам / Д. С. Лаврова, Д. П. Зегжда, Е. А. Зайцева // Вопросы кибербезопасности. – 2019. – № 2(30). – С. 13-20. DOI:10.21681/2311-3456-2019-2-13-20
3. Дойникова Е. В. Оценивание защищенности и выбор контрмер для управления кибербезопасностью / Е. В. Дойникова, И. В. Котенко. М.: РАН, 2021. — 184 с. ISBN 978-5-907366-23-7.
4. Середкин С. П. Моделирование угроз безопасности информации на основе банка угроз Федеральной службы по техническому и экспортному контролю России / С. П. Середкин // Информационные технологии и математическое моделирование в управлении сложными системами. – 2022. – № 1(13). – С. 43-54.
5. Сердечный А. Л. Моделирование, анализ и противодействие сценариям компьютерных атак, реализуемых группировкой APT29 в распределенных компьютерных системах / А. Л. Сердечный, П. С. Краюшкин, М. А. Тарелкин, Ю. К. Язов // Информация и безопасность. – 2021. – Т. 24. – № 1. – С. 83-92.
6. Сердечный А. Л. Моделирование, анализ и противодействие сценариям компьютерных атак, реализуемых группировкой APT3 в распределенных компьютерных системах / А. Л. Сердечный, А. В. Айдаркин, М. А. Тарелкин, А. Е. Дешина // Информация и безопасность. – 2021. – Т. 24. – № 1. – С. 35-46.
7. Будников С. А. Моделирование APT-атак, эксплуатирующих уязвимость Zerologon / С. А. Будников, Е. Е. Бутрик, С. В. Соловьев // Вопросы кибербезопасности. – 2021. – № 6(46). – С. 47-61. DOI:10.21681/2311-3456-2021-6-47-61
8. Егошин Н. С. Модель типовых угроз безопасности информации, основанная на модели информационных потоков / Н. С. Егошин // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2021. – Т. 24. – № 3. – С. 21-25.
9. Кондаков С. Е. Модель процесса проведения компьютерных атак с использованием специальных информационных воздействий / С. Е. Кондаков, И. С. Рудь // Вопросы кибербезопасности. – 2021. – № 5(45). – С. 12-20. DOI:10.21681/2311-3456-2021-5-12-20
10. Ерышов В. Г. Моделирование процесса защиты объектов критической информационной структуры промышленных предприятий от компьютерных атак / В. Г. Ерышов, Р. Д. Куликов // Морской вестник. – 2021. – № 1(77). – С. 91-96.
11. Хованских С. А. Методика защиты распределенных вычислений в многоагентной системе / С. А. Хованских, В. А. Литвиненко, В. С. Хованскова // Известия ЮФУ. Технические науки. – 2019. – № 4(206). – С. 68-80.
12. Дойникова Е. В. Оценка защищенности компьютерных сетей на основе метрик CVSS / Е. В. Дойникова, А. А. Чечулин, И. В. Котенко // Информационно-управляющие системы. – 2017. – № 6(91). – С. 76-87.
13. Пучков В. В. Анализ защищенности киберфизических систем с использованием графов атак / В. В. Пучков, И. В. Котенко // Информационная безопасность регионов России (ИБРР-2021) : Материалы конференции, Санкт-Петербург, 27–29 октября 2021 года. – Санкт-Петербург: Региональная общественная организация “Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления”, 2021. – С. 98-100.
14. Левшун Д. С. Проблемные вопросы информационной безопасности киберфизических систем / Д. С. Левшун, Д. А. Гайфулина, А. А. Чечулин, И. В. Котенко // Информатика и автоматизация. – 2020. – Т. 19. – № 5. – С. 1050-1088.
15. Калашников, А.О. Модель управления информационной безопасностью критической информационной инфраструктуры на основе выявления аномальных состояний (часть 1) / А.О. Калашников, Е.В. Аникина // Информация и безопасность. – 2018. – Т. 21. – № 2. – С. 145-154.
16. Калашников, А.О. Модели количественного оценивания компьютерных атак / А.О. Калашников, К.А. Бугайский, Е.В. Аникина // Информация и безопасность. – 2019. – Т. 22. – № 4. – С. 517-538.
17. Вдовикина Н.В. Операционные системы: взаимодействие процессов / Н.В. Вдовикина, И.В. Машечкин, А.Н. Терехин, А.Н. Томилин. – М.: МАКС Пресс, 2008. 216 с.

A MODEL FOR ASSESSING THE SECURITY OF A COMPLEX NETWORK (PART 1)

Kalashnikov A.O.[3], Bugajskij K.A.[4]

Purpose of the article: *development of mechanisms for evaluating the actions of agents of complex information systems from the point of view of information security.*

Research method: *game-theoretic models using stochastic modeling methods.*

The result: *the description of the subject area of application of the model is given, it is shown that the actions of the violator and defender can be considered from the point of view of obtaining and further escalation of access rights on the objects of the information system. It is shown that the model of information confrontation between the defender and the violator can be represented by the triple "graph, agent, rules". The definition of the basic terms and concepts of the model is given. The basic principles of the model functioning have been developed. The possibility of implementing calculations of the results of agents' activities and the results of the game in the conditions of information uncertainty is shown. A list of basic values of the model is defined that allow calculating the costs and winnings of the participants of the game. The basic rules for calculating costs and winnings have been developed. The input parameters of the model that are set during its initialization are defined. The role and place of "playing with nature" for calculating the basic values of the model are shown.*

Keywords: *information security model, assessment of complex systems, game-theoretic approach, information uncertainty, playing with nature.*

References

1. Kalashnikov A.O. Infrastruktura kak kod: formiruetsya novaya real'nost' informacionnoj bezopasnosti / A.O. Kalashnikov, K.A. Bugajskij // Informaciya i bezopasnost'. 2019. T. 22. № 4. S. 495-506.
2. Lavrova D. S. Modelirovanie setevoj infrastruktury' slozhny'x ob"ektov dlya resheniya zadachi protivodejstviya kiberatakam / D. S. Lavrova, D. P. Zegzhda, E. A. Zajceva // Voprosy' kiberbezopasnosti. – 2019. – № 2(30). – S. 13-20. DOI:10.21681/2311-3456-2019-2-13-20
3. Dojnikova E. V. Ocenivanie zashhishhennosti i vy'bor kontrmer dlya upravleniya kiberbezopasnost'yu / E. V. Dojnikova, I. V. Kotenko. M.: RAN, 2021. — 184 s., ISBN 978-5-907366-23-7.
4. Seredkin S. P. Modelirovanie ugroz bezopasnosti informacii na osnove banka ugroz Federal'noj sluzhby' po texnicheskomu i e'ksportnomu kontrolyu Rossii / S. P. Seredkin // Informacionny'e texnologii i matematicheskoe modelirovanie v upravlenii slozhny'mi sistemami. – 2022. – № 1(13). – S. 43-54.
5. Serdechny'j A. L. Modelirovanie, analiz i protivodejstvie scenariyam komp'yuterny'x atak, realizuemy'x gruppirovkoj APT29 v raspredelenny'x komp'yuterny'x sistemax / A. L. Serdechny'j, P. S. Krayushkin, M. A. Tarelkin, Yu. K. Yazov // Informaciya i bezopasnost'. – 2021. – T. 24. – № 1. – S. 83-92.
6. Serdechny'j A. L. Modelirovanie, analiz i protivodejstvie scenariyam komp'yuterny'x atak, realizuemy'x gruppirovkoj APT3 v raspredelenny'x komp'yuterny'x sistemax / A. L. Serdechny'j, A. V. Ajdarkin, M. A. Tarelkin, A. E. Deshina // Informaciya i bezopasnost'. – 2021. – T. 24. – № 1. – S. 35-46.
7. Budnikov S. A. Modelirovanie APT-atak, e'kspluatiruyushhix uyazvimost' Zerologon / S. A. Budnikov, E. E. Butrik, S. V. Solov'ev // Voprosy' kiberbezopasnosti. – 2021. – № 6(46). – S. 47-61. DOI:10.21681/2311-3456-2021-6-47-61
8. Egoshin N. S. Model' tipovy'x ugroz bezopasnosti informacii, osnovannaya na modeli informacionny'x potokov / N. S. Egoshin // Doklady' Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioe'lektroniki. – 2021. – T. 24. – № 3. – S. 21-25.
9. Kondakov S. E. Model' processa provedeniya komp'yuterny'x atak s ispol'zovaniem special'ny'x informacionny'x vozdejstvij / S. E. Kondakov, I. S. Rud' // Voprosy' kiberbezopasnosti. – 2021. № 5(45). S. 12-20. DOI:10.21681/2311-3456-2021-5-12-20
10. Ery'shov V. G. Modelirovanie processa zashhity' ob"ektov kriticheskoj informacionnoj struktury' promy'shlenny'x predpriyatij ot komp'yuterny'x atak / V. G. Ery'shov, R. D. Kulikov // Morskoj vestnik. – 2021. – № 1(77). – S. 91-96.

3 Andrey O. Kalashnikov, Dr.Sc., Chief Scientist of the Laboratory «Complex networks» Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. E-mail: aokalash@ipu.ru

4 Konstantin A. Bugajskij, Junior Researcher of the Laboratory «Complex networks» Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. E-mail: kabuga@ipu.ru

11. Xovanskov S. A. Metodika zashhity' raspredelenny'x vy'chislenij v mnogoagentnoj sisteme / S. A. Xovanskov, V. A. Litvinenko, V. S. Xovanskova // Izvestiya YuFU. Texnicheskie nauki. – 2019. – № 4(206). S. 68-80.
12. Dojnikova E. V. Ocenka zashhishhennosti komp'yuterny'x setej na osnove metrik CVSS / E. V. Dojnikova, A. A. Chechulin, I. V. Kotenko // Informacionno-upravlyayushhie sistemy'. – 2017. – № 6(91). S. 76-87.
13. Puchkov V. V. Analiz zashhishhennosti kiberfizicheskix sistem s ispol'zovaniem grafov atak / V. V. Puchkov, I. V. Kotenko // Informacionnaya bezopasnost' regionov Rossii (IBRR-2021) : Materialy' konferencii, Sankt-Peterburg, 27–29 oktyabrya 2021 goda. – Sankt-Peterburg: Regional'naya obshhestvennaya organizaciya "Sankt-Peterburgskoe Obshhestvo informatiki, vy'chislitel'noj texniki, sistem svyazi i upravleniya", 2021. – S. 98-100.
14. Levshun D. S. Problemny'e voprosy' informacionnoj bezopasnosti kiberfizicheskix sistem / D. S. Levshun, D. A. Gajfulina, A. A. Chechulin, I. V. Kotenko // Informatika i avtomatizaciya. – 2020. – T. 19. – № 5. – S. 1050-1088.
15. Kalashnikov, A.O. Model' upravleniya informacionnoj bezopasnost'yu kriticheskoj informacionnoj infrastruktury' na osnove vy'yavleniya anomal'ny'x sostoyanij (chast' 1) / A.O. Kalashnikov, E.V. Anikina // Informaciya i bezopasnost'. – 2018. – T. 21. – № 2. – S. 145-154.
16. Kalashnikov, A.O. Modeli kolichestvennogo ocenivaniya komp'yuterny'x atak / A.O. Kalashnikov, K.A. Bugajskij, E.V. Anikina // Informaciya i bezopasnost'. – 2019. – T. 22. – № 4. – S. 517-538.
17. Vdovikina N.V. Operacionny'e sistemy': vzaimodejstvie processov / N.V. Vdovikina, I.V. Mashechkin, A.N. Terexin, A.N. Tomilin. – M.: MAKS Press, 2008. 216 s.