ВВЕДЕНИЕ

История человеческой цивилизации — это непрерывная череда освоений новых пространств. Именно благодаря этому мы из разрозненных племён превратились в глобальную социальную систему, расположенную не только на суше, но и в космическом пространстве. Покорение морей и океанов позволило связать население различных континентов. Освоение воздушного пространства дало возможность быстрого перемещения практически во всякий уголок планеты, а космическая одиссея открыла способность передачи сообщений практически в любую точку Земли. Кроме того, благодаря развитию цифровых технологий, человечество породило принципиально новую среду, названную киберпространством и обладающую особыми свойствами.

Столь масштабная экспансия принципиально не могла быть эффективной без создания в отношении осваиваемых сред обозримых и наполненных сущностью (для исследователя) образов, где добытые сведения о интересующих пространствах «натягивались» на плоскостные (карты), сферические (глобус) и другие поверхности, удобные для человеческого восприятия. Подобное макетирование пространственных объектов первоначально вошло в пользование для исследования природных, т. е. геологических и космологических сред. Теперь же очередь дошла и до рукотворного киберпространства, виртуально пронизывающего все вышеуказанные среды.

Ориентирование в каждой из упомянутых сред объективно требует наличия соответствующего навигационного инструмента — карты, которая бы точно описывала нужные особенности исследуемого пространства. Так, для осознанного перемещения по суше требуются географические карты, для судоходства нужны речные, морские и океанические карты, для движения самолётов — воздушные карты, а вывод спутника в нужную точку невозможен без астрономических карт. Увы, для киберпространства подобный инструмент в настоящий момент отсутствует, что особенно критично в условиях колоссальных опасностей, которые в нем подстерегают личность, общество и государство.

В этой связи в монографии подробно рассмотрены понятие «киберпространство» и его свойства прежде всего в контексте решения задач защиты информации и обеспечения информационной безопасности, где развитие информационных технологий привело к взрывному возрастанию сложности технических систем, что отражается на эффективности решения этих задач. Так, например, для оценки угроз безопасности для информационной системы требуется рассматривать тысячи различных способов осуществления компьютерных атак и мер защиты от них. Реализация таких угроз во многом связана с уязвимостями программного обеспечения, выявление которых требует от эксперта знания особенностей информационных технологий, а также специфики организации киберпреступности, которая за счёт технологической децентрализации и криптографии приобрела сегодня новые качества и возможности.

В области информационной безопасности также никто не снимал «проклятие размерности». В условиях недостаточной образованности населения, высокой доступности технологий конструирования «фейков» и масштабов возможностей их распространения, мониторинг защищенности социо-информационного пространства превращается в гиперобъемную задачу, решение которой без средств искусственного интеллекта уже не представляется возможным.

В настоящий момент разрешение данных проблем в основном пытаются осуществить за счёт использования технологий машинного обучения, позволяющих во многом автоматизировать предварительную обработку сведений. Однако интерпретация и оценка качества результатов такого анализа по-прежнему возлагается на человека и требует от него высокой компетентности и глубоких знаний предметной области с гигантским объёмом данных. Причём количество этих областей защиты информации и обеспечения информационной безопасности, а также их терминологическое многообразие увеличиваются по экспоненциальному закону и требуют изменения подхода в образовании и систематизации наколенных знаний.

В этом контексте настоящая монография презентует методологию, позволяющую приблизиться к разрешению обозначенных противоречий за счёт создания методической и инструментальной основы картографирования защищаемого киберпространства через понятие «информационная карта», которое вводится как обобщение термина «географическая карта», используемого для моделирования географических объектов. Информационные карты подобно географическим позволяют проводить экспертный анализ большого объёма данных в соответствии с чёткими обоснованными правилами.

Отсюда для создания инструментальной основы вводится новый класс информационных систем, названных информационно-картографическими, где исследователю становятся доступны такие функции, как информационная навигация, многоуровневое масштабирование, сравнение информационных объектов в различных контекстах, а самое главное — возможность наглядного определения близости между информационными объектами на основании их расположения на информационной карте (подобно тому, как при помощи расстояния между объектами на географической карте определяется их близость в физическом пространстве).

Идея возможного использования метафоры ландшафта и карт для визуализации информационных объектов и процессов относительно не нова, однако до настоящего времени не были предложены обоснованные правила построения и анализа информационных карт. Вместе с тем формирование таких правил возможно за счёт объединения знаний в рамках следующих направлений: теория сетей, картография и геоинформационные системы, научная визуализация данных, экспертные системы и базы знаний, численные методы и методы машинного обучения, управление рисками нарушения информационной безопасности и т. п.

Поэтому в настоящей монографии предлагается система методов построения и анализа информационных карт для решения задач в разноплановых отраслях: картографической разведки, планирования операций, мониторинга обстановки, представления знаний и др., включая применение цифровых технологий для создания и использования информационно-картографических систем, их апробацию при решении спектра задач защиты информации и обеспечения информационной безопасности.

В первой главе раскрывается суть понятия «киберпространство» и даётся его характеристика в качестве объекта исследования и защиты. Рассматриваются информационный, технический, социальный, виртуальный, пространственный, глобальный и регуляторный аспекты киберпространства на различных этапах его развития. Поднимаются вопросы о расположении киберпространства и формах его представления с целью понимания протекающих в нем процессов, которые оказывают существенное влияние на безопасность личности, общества и государства. Определяются проблемы исследования защищаемого киберпространства, которые связаны с неопределённостью в отношении зон влияния и правил его регулирования, а также его колоссальными размерами, из-за которых требуется реализация новых подходов его мониторинга. Даётся характеристика основных подходов к исследованию киберпростран-

ства, среди которых шаблонно-онтологический, теоретико-игровой, сетевой, географический и картографический, а также формулируются их возможности и ограничения. Осуществляется постановка задач исследования киберпространства с использованием картографической методологии.

Вторая глава посвящена формализации основных принципов картографического анализа защищаемого киберпространства, где информационная карта представляет собой обобщение понятия карта, используемого в различных науках. В связи рассмотрены категории задач, решаемых с помощью информационных карт, и раскрыты основные процедуры построения и анализа информационной карты, выполнение которых носит циклический характер, связанный с необходимостью уточнения построенной карты в результате получения новых знаний в ходе её анализа. В главе также раскрыты основные методические и инструментальные аспекты информационного картографирования и определён круг проблемных вопросов, связанных с применением методики картографического анализа защищаемого киберпространства.

В третьей главе представлены математические основы картографии защищаемого киберпространства, включающие модели информационной карты и процессов её исследования. Рассматриваются методы многомерного шкалирования для снижения размерности при отображении многомерных сведений в двух- или трёхмерное пространство, используемого для визуализации информационной карты. Приводятся показатели оценки искажений, связанных со снижением размерности. Даётся характеристика основных алгоритмов автоматизации процедур информационно-картографического исследования, к которым относятся алгоритмы сетевого анализа, а также проекционные и интерполяционные алгоритмы, применяемые в геоинформационных системах.

В четвёртой главе рассматриваются технологии, необходимые для создания информационно-картографических систем. Данный класс программных систем вводится для обозначения средств автоматизации работы с информационными картами и обобщает классы таких средств, как геоинформационные системы (автоматизация процессов обработки геопространственных данных) и средства разведки по открытым источникам (сбор из открытых источников, интеграция и обработка связанных данных). Предлагаются различные варианты архитектуры построения таких средств. Даётся характеристика технологий хранения информационных карт, визуализации защищаемого киберпространства и анализа связанных и геопространственных данных.

Пятая глава посвящена методам и способам картографирования защищаемого киберпространства, к которым относятся методы построения и анализа информационных карт. При построении информационной карты применяются методы моделирования данных и сбора исходных данных, методы визуализации и актуализации информационных карт. Для анализа информационных карт используются методы картографического и сетевого анализа. Также в пятой главе рассматриваются особенности применения данных методов с учётом масштаба, модели данных информационной карты, а также специфики задач картографического исследования.

В завершающей главе монографии демонстрируется практическое применение разработанной методологии на примерах решения актуальных задач обеспечения безопасности защищаемого киберпространства. Самой важной для защищаемого киберпространства является задача построения генеральной карты, на которой можно комплексно представить все его аспекты, определить зоны влияния субъектов киберпространства, ограничить защищаемую область, где должна поддерживаться безопасность всех участников, имеющих доступ к ней. Также в главе рассмотрены пути построения такой карты, перспективы использования информационных карт в контексте задач ведения кибервойны, практические примеры из области защиты информации и обеспечения информационной безопасности, для которых применение информационной карты даёт преимущества по сравнению с традиционными подходами (оценка рисков реализации информационных угроз, расследование компьютерных преступлений, мониторинг компьютерных атак и др.).

В приложения к монографии сведены актуальные результаты применения методологии картографирования защищаемого киберпространства. Так, в приложении 1 проиллюстрировано её использование в библиометрических сетях, что позволило разработать методику поиска научных публикаций (картографический поиск) в целях повышения скорости и качества анализа источников по любой теме исследований. При этом продемонстрирован подход к изучению творческих коллективов, который позволяет обнаруживать авторов, занимающихся тематическими исследованиями, а также выявлять и анализировать развитие научных школ. Демонстрация методики реализована на примере научных школ, сложившихся в области защиты информации и обеспечения информационной безопасности. В приложении 2 рассмотрены средства количественной оценки эффективности информационных карт, а в приложении 3 монографии представлены результаты разработки «Системы картографирования рисков защищаемого киберпространства».

Полноцветные иллюстрации информационных карт, приведённые в настоящей монографии, читатель может изучить по соответствующим ссылкам в тексте.

Авторы выражают глубокую благодарность кибердружине Воронежского государственного технического университета, члены которой в рамках проекта «Безопасный Интернет» активно способствовали подготовке материалов для настоящей монографии.