Введение

Интенсивное развитие и использование современных информационно-коммуникационных технологий (ИКТ) для обработки цифровой информации привели к серьезным качественным изменениям в экономической, социально-политической и духовной сферах жизни общества. Этот феномен большой зависимости от ИКТ и их резко возрастающего влияния на формирование цифрового общества XXI века был впервые отмечен в «Окинавской Хартии глобального информационного общества», принятой в 2000 г. лидерами «восьмерки» [1]. В 2016 г. в «Доктрине информационной безопасности Российской Федерации» также отмечалось, что эти технологии «приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства» [2].

В России в рамках реализации Указа Президента Российской Федерации № 204 «О национальных целях и стратегических задачах развития Российской Федерации (РФ) на период до 2024 года» [3] была принята Национальная программа «Цифровая экономика Российской Федерации» [4], одна из трех целей которой — «создание устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных, доступной для всех организаций и домохозяйств». Для обеспечения ее решения в Национальный проект включен Федеральный проект «Информационная безопасность», который полностью согласуется с направлением обеспечения информационной безопасности (ИБ) в области государственной и общественной безопасности РФ, сформулированным в [2] как «повышение безопасности функционирования объектов информационной инфраструктуры, в том числе в целях обеспечения устойчивого взаимодействия государственных органов, недопущения иностранного контроля за функционированием таких объектов, обеспечение целостности, устойчивости функционирования и безопасности единой сети электросвязи Российской Федерации, а также обеспечение безопасности информации, передаваемой по ней и обрабатываемой в информационных системах на территории Российской Федерации». В основе названной инфраструктуры лежит информационно-телеком-

муникационная система [5], которая базируется на информационно-телекоммуникационной сети (ИТКС) — технологической системе (ТС), предназначенной для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники (СВТ) [6, статья 2].

Согласно Федеральному закону № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», к объектам критической информационной инфраструктуры (КИИ) относятся ИТКС, информационные системы (ИС), автоматизированные системы управления (АСУ) субъектов КИИ, а также сети электросвязи, используемые для организации взаимодействия таких объектов. Субъекты КИИ — государственные органы и учреждения, российские юридические лица и (или) индивидуальные предприниматели (далее — организация), которым на праве собственности, аренды или на ином законном основании принадлежат ИС, ИТКС, АСУ, функционирующие в различных сферах деятельности и областях промышленности, а также российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей [7, статья 2]. Следовательно, для ИТКС как неотъемлемой части обеспечения деятельности организаций необходимо обеспечить функциональную устойчивость и ИБ их информационных ресурсов и предоставляемых услуг.

В то же время в последнее десятилетие риски нарушения безопасности для объектов КИИ, включая ИТКС ее субъектов, приобрели статус компонентов системного риска. В качестве основных причин данной тенденции можно выделить, в первую очередь, сложность и разнородность ИТКС разных субъектов по функциям, структуре и организационно-правовым формам, растущую роль различных технологий в предоставлении услуг и все большую зависимость последних от имеющих различные уязвимости ИКТ, усиливающуюся взаимозависимость всех участников информационных взаимодействий, а также рост сложности, широкой направленности и разнообразия компьютерных атак и появление новых категорий злоумышленников и целей, которые они преследуют. Многочисленные ежегодные исследования в области ИБ ИТКС показывают, что стратегии обеспечения ИБ, которые традиционно были основаны на соблюдении нормативных и правовых требований и ограничивались лишь «защитой периметра», не успевают за растущим количеством и все более изощренными методами, применяемыми злоумышленниками. В качестве примеров подобной тенденции можно привести атаки на системы Интернета вещей (*Internet of Things, IoT*) и *APT*-атак (*Advanced Persistent Threats, APTs*), направленные на цели

определенной категории (как правило, делового или политического характера), промышленный шпионаж и кражу бизнес-информации. Часто злоумышленники сначала получают доступ к плохо защищенным серверам и компьютерам пользователей, а затем с них производят атаки на системы по всему миру. Они умеют осторожно тестировать защиту ИТКС, избегая обнаружения, и, найдя уязвимости, используют их для достижения своих целей. Например, прибегают к целевому фишингу (*spear phishing*) в отношении группы пользователей с определенным сходством и, как результат, незаконным путем получают необходимую информацию от сотрудников компаний. Для внедрения вредоносного кода могут использоваться как технические средства, так и социальная инженерия (*social engineering*). Например, статистика атак за 2020 г. от аналитической компании Hackmaggedon показывает, что большинство из них связаны с распространением вредоносного программного обеспечения (ПО) (39,3 %), похищением учетных записей (16,7 %), целенаправленными атаками (10,7 %), внедрением вредоносных скриптов (3,7 %), спамом (1,8 %), *DDoS*-атаками (*Distributed Denial of Service*) (1,7 %), созданием поддельных страниц (1,5 %) и неверных конфигураций (1,1 %) [8].

Одновременно с этим увеличивается число потенциальных точек проникновения в ИТКС, по которым злоумышленники наносят «точечные удары», приводящие к утечке конфиденциальной информации, загрузке приложений через почтовые сообщения, несанкционированному переводу денежных средств и т. д. Системотехническая основа современных ИТКС может включать элементы, которые входят в состав систем общего пользования (систем облачных вычислений, различных хранилищ и центров обработки данных (ЦОД) с множеством ИС и т. п.), что несет повышенную угрозу ее ИБ. Программируемые сети, управляемые ПО, а не аппаратными средствами, обладают рядом уязвимостей, а также создают задержки в обработке трафика управления передачей данных, что позволяет реализовывать компьютерные атаки на уровне ПО. Пятое поколение мобильных сетей (сети 5G), как и любое новшество, кроме пользы содержит в себе множество возможностей, которыми может воспользоваться злоумышленник, и т. п. Проиллюстрируем один аспект незащищенности облачных хранилищ, открывающий путь к атакам и представленный в обзоре за 2020 г. компанией Verizon [9]: 22 % нарушений были связаны с облачными активами, а 43 % — с веб-приложениями, в 71 % зарегистрированных инцидентов были затронуты локальные активы; 70 % атак было совершено внешними нарушителями, организованная преступность имела отношение к 55 %

из них; 81 % нарушений были обнаружены в течении нескольких дней или раньше; у 58 % жертв были скомпрометированы личные данные; 86 % нарушений имели финансовые мотивы.

В целях обеспечения ИБ в соответствии с требованиями к созданию систем безопасности таких объектов и обеспечению их функционирования, утвержденными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ РФ, субъект КИИ создает систему безопасности объекта и обеспечивает ее функционирование [7, статья 10]. При этом безопасность КИИ, включающей ИТКС разных субъектов — это состояние защищенности КИИ, обеспечивающее ее функциональную устойчивость при проведении в отношении нее компьютерных атак [7, статья 2]. Наравне с законностью, к принципам обеспечения безопасности КИИ относятся непрерывность и комплексность этого процесса и приоритет предотвращения компьютерных атак [7, статья 4].

Реализуемые в настоящее время реактивные меры обеспечения ИБ для информационных ресурсов ИТКС организаций с целью минимизации времени их восстановления (длительности реагирования) после прерываний, вызванных инцидентами ИБ, были разработаны два-три десятилетия назад. В 2005–2006 гг. компанией Cisco Systems была впервые озвучена идея разработки центра мониторинга безопасности (ЦМБ) (*Security Operations Center, SOC*) [10–12], которому в русскоязычных публикациях долгое время соответствовали разные термины типа «система централизованного мониторинга ИБ», или «центр координации деятельности по ИБ» [13], «координирующий центр мониторинга ИБ», или «ситуационный центр мониторинга ИБ» (например, [14, 15]). Основными целями разворачивания ЦМБ Cisco определил управление средствами защиты информации (СЗИ) в сетях (например, виртуальными частными сетями, межсетевыми экранами, системами обнаружения и предотвращения вторжений, системами отражения *DDoS*-атак, решениями для борьбы с вредоносным кодом, вирусами и шпионскими программами) и мониторинг их состояния в режиме реального времени, а также анализ записей в журналах регистрации событий [16], сведений об уязвимостях, информации о ресурсах и предупреждений об опасности.

В то же время дальнейшего развития требует качество управления сетевой безопасностью в ЦМБ, поскольку оно существенно отстает от требуемого сегодня уровня — ЦМБ первого поколения не были рассчитаны на сложную корреляцию и аналитику всех происходящих в ИТКС событий в определенном контексте как основы полноценного управления, а не просто мониторинга ИБ. Результатом является неудовлетворительное время обнаружения инцидентов

ИБ. К сожалению, единой общемировой статистики по его оценке не существует — данные в отчетах разных исследовательских компаний существенно различаются. Но общие тенденции выявить можно. Так, например, известный в мире ИБ центр Ponemon Institute (США) в отчете 2019 г. отмечает, что компании необходимо в среднем 276 дней (против 197 в 2018 г.) для выявления инцидентов, связанных с утечкой данных [17]. Некоторые исследования показывают, что большинство инсайдерских атак обнаруживаются в течение нескольких минут (22 % опрошенных), часов (28 %) или одного дня (26 %) (Crowd Research Partners 2018 Insider Threat Report, [18]). Другой отчет показывает, что для выявления такого нарушения требуется от нескольких месяцев (30 % опрошенных) до нескольких лет (40 %) (Verizon 2019 Insider Threat Report: Executive Summary, [19]). И это при том, что, согласно Website hacking statistics of 2020 [20], хакеры атакуют каждые 39 секунд, в среднем 2244 раза в день; крадут 75 записей каждую секунду (источник: Breach Level Index); в среднем взламывают 30000 новых веб-сайтов каждый день (источник: Forbes). Они ежедневно создают 300000 новых вредоносных программ (источник: McAfee). 73 % хакеров заявили, что традиционный межсетевой экран и антивирусная защита неактуальны или устарели (источник: Thycotic.com).

Из вышеизложенного очевиден вывод, что в настоящее время актуален поиск решения для построения центра управления ИБ для ИТКС (центра управления сетевой безопасностью), за счет которого достигается соблюдение для ИТКС организации соответствующих требований по обеспечению ее ИБ (например, для субъекта КИИ в соответствии с присвоенной ему категорией значимости [21]). Такое решение обеспечит *информационную защищенность ИТКС организации* — такую ее способность, при которой в едином информационной пространстве (ЕИП) организации создана адекватная защищенная среда функционирования ИТКС, обеспечивающая необходимый уровень ИБ для получения (поиска и сбора), обработки, хранения, распространения (передачи и предоставления) и уничтожения информации. Обобщив определения из [2, 5–7, 22], определим *ИБ ИТКС организации* как состояние защищенности ТС организации, предназначенных для обработки и передачи по линиям связи информации, доступ к которой осуществляется с использованием современных информационных технологий (ИТ), СВТ и средств связи, включающее безопасность информационных ресурсов и предоставляемых услуг и обеспечивающее функциональную устойчивость ИТКС в штатном режиме и в условиях угроз ИБ (в условиях направленных на него компьютерных атак, при сбоях по-

вышенной степени серьезности и в условиях чрезвычайных ситуаций) в ЕИП организации. При этом уровень риска нарушения осуществления деятельности организации с использованием ИТКС и уровень риска нарушения свойств ИБ информационных ресурсов ИТКС на всех стадиях их жизненного цикла приемлемы как для их пользователя, так и владельца. Защищенность достигается обеспечением совокупности свойств ИБ — конфиденциальности, целостности, доступности, подлинности, подотчетности, неотказуемости и достоверности, приоритетность которых определяется значимостью информации для интересов (целей) организации.

Требуемое решение должно обеспечить ИБ ИТКС организации на основе предоставления следующих возможностей:

1) консолидированное (единое) управление ИБ ИТКС для недопущения несанкционированных воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование ИТКС;

2) не только предотвращение неправомерных действий, включая доступ, уничтожение, модифицирование, блокирование, копирование, предоставление и распространение в отношении информации, обрабатываемой ИТКС, но и *упреждающее управление сетевой безопасностью ИТКС*, основанное на принятии решений в отношении возможных инцидентов ИБ до их проявления, направленном на предотвращение и минимизацию их последствий за счет постоянного интеллектуального анализа в определенном контексте всех консолидированных (совместно рассматриваемых и анализируемых) данных о происходящих в ИТКС событиях, имеющих отношение к ИБ, прогнозирования развития ситуации и своевременной установки «барьеров защиты» на пути распространения таких действий;

3) обеспечение неотъемлемого свойства ИТКС — ее функциональной устойчивости как способности регулировать функционирование с целью поддержания выполнения операций при ожидаемых условиях и в условиях ужесточения требований, нарушений и непредвиденных обстоятельств «в малом», когда достаточно малое отклонение режима работы от исходного (установившегося) с течением времени уменьшается и функционирование ИТКС возвращается в исходное состояние, и «в большом», когда функционирование ИТКС, получив достаточно большое начальное отклонение, возвращается в исходное состояние после прекращения действия компьютерной атаки [23, 24];

4) непрерывное и продуктивное взаимодействие с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ (ГосСОПКА [25]).

Актуальность исследования определяется необходимостью эффективного и результативного противодействия компьютерным атакам в ИТКС, масштаб и сложность которых постоянно растет при совершенствовании способов реализации с учетом развития информационно-коммуникационных технологий (ИКТ), когда при применении традиционных стратегий и систем обеспечения ИБ, основанных на принципе реагирования, а не упреждения угроз и инцидентов ИБ, невозможно обеспечить требуемый уровень ИБ ИТКС организации.

Проведенный анализ показывает необходимость исследования и разработки научно обоснованной методологии и принципов построения организационно-технических средств обеспечения ИБ для ИТКС. Поэтому *объектом исследования* определена ИТКС организации как важнейший объект субъектов КИИ с точки зрения необходимости защиты ее информационных ресурсов на всех стадиях их жизненного цикла (создания, сбора, обработки, накопления, хранения, поиска, распространения, использования и уничтожения).

Для упреждающего управления сетевой безопасностью ИТКС требуется использование новейших методов обработки и хранения информации. Только при таком походе удастся обеспечить возможность синтезировать новые знания о будущих угрозах ИБ для ИТКС и обоснованно прогнозировать развитие событий в области ИБ ИТКС. Это и определяет *предмет исследования* — построение специализированных центров, обеспечивающих информационную защищенность передаваемых по таким сетям данных на всех стадиях жизненного цикла ИТКС в условиях угроз ИБ в ЕИП организации, а также при возникновении отказов в работе, требующих реструктуризации системо-технической составляющей ИТКС, за счет создания в ее составе с применением современных интеллектуальных подходов типового специализированного структурного элемента — «Центра интеллектуального управления сетевой безопасностью» (ЦИУСБ). Первоочередной целью развертывания ЦИУСБ является предоставление организации возможностей по организации непрерывных процессов предотвращения, выявления и оперативного реагирования на события ИБ, происходящие в ИТКС в реальном времени, а также прогнозированию и предупреждению компьютерных атак на защищаемые объекты ИТКС на всех стадиях их жизненного цикла на основе своевременного интеллектуального анализа данных об этих событиях и выявленных требующих немедленной корректировки тенденций в уровне ИБ ИТКС в сравнении с заданными критериями.

Проведенные в монографии исследования решают *научную проблему*, состоящую в формировании научной основы обеспечения

информационной защищенности и функциональной устойчивости сложных систем класса ИТКС в штатном режиме и в условиях угроз ИБ (в условиях направленных на него компьютерных атак, при сбоях повышенной степени серьезности и в условиях чрезвычайных ситуаций) в ЕИП организации, что может быть достигнуто в результате разработки методологии и принципов построения специализированного структурного элемента ИТКС организации — ЦИУСБ, призванного осуществлять упреждающее управление сетевой безопасностью ИТКС на всех стадиях жизненного цикла ее информационных ресурсов за счет прогнозирования развития событий в области ИБ ИТКС и применения в ЦИУСБ для достижений этих целей интеллектуальных подходов обработки больших относящихся к ИБ ИТКС данных. Непременным условием результативного функционирования ЦИУСБ для оперативной коррекции текущего уровня ИБ ИТКС в ЕИП организации будет являться его обязательное вхождение в состав общей системы обеспечения ИБ (СОИБ). ЦИУСБ как ее важнейшая часть должен быть жестко связан с СОИБ ИТКС и влиять на ее развитие и совершенствование, для чего требуется комплексное обеспечение ИБ всех элементов ИТКС и разработка образовательных аспектов в части обучения разработчиков и персонала ЦИУСБ тому, как квалифицированно создавать, внедрять и эксплуатировать ЦИУСБ. Внедрение ЦИУСБ позволит устранить имеющееся в настоящее время острое противоречие между, с одной стороны, невозможностью избежать компьютерных атак в ИТКС, осуществляемых искушенными злоумышленниками, имеющими доступ к новейшим ИКТ, учитывая тенденцию к постоянному росту масштаба и сложности этих атак, и с другой стороны, использованием в этих условиях для обеспечения на одинаково высоком уровне информационной защищенности и, следовательно, функциональной устойчивости современных ИТКС устаревших стратегий и СОИБ, основанных на принципе реагирования, а не упреждения угроз и инцидентов ИБ, и, как следствие, обеспечивающих недостаточный уровень ИБ ИТКС организации.

Рассматриваемая проблема обеспечения ИБ в вычислительных сетях находится в центре внимания специалистов уже около 40 лет, с момента появления Интернет-протокола (*Internet Protocol, IP*) в качестве стандартного сетевого протокола ARPANET с 1982 г. В настоящее время известны подходы и лучшие практики к обеспечению ИБ сетей, которые были взяты за отправную точку данной работы. Исследованиями в области защищенности ИС и систем мониторинга ИБ занимались такие отечественные и зарубежные ученые, как П.Д. Зегжда, О.Б. Макаревич, А.А. Малюк, Е.Б. Белов, В.В. Романов, А.В. Лукацкий, А.К. Скуратов, И.В. Щербакова,

А.В. Андронов, А.В. Мамаев, А.А. Лавров, К.Г. Абрамов, С.Ю. Исхаков, А.В. Гирик, С.И. Штеренберг, Т.Р. Кашаев, Авад Маркад Лебнан, M. Basseville, A. Benveniste, R. Bidou, M. Bishop, H.R. Debar, R. Marchan, L.A. Johnson, J. Myers, V. Paxson, D. Shin, F.W. Feather, M. Thottan, C. Ji G. Wang, H. Zhang и другие. Наиболее близкими к теме данного исследования являются следующие работы: по методическому и информационно-аналитическому обеспечению и взаимодействию для ситуационного управления защищенностью АС и ситуационно-аналитических центров — С.В. Соловьев [26], А.В. Ламонов [27], А.А. Лукашин [28], В.М. Попов [29] и А.П. Глухов [30]; по вопросам адаптивного управления ИБ — М.В. Калинин [31], А.С. Исаев [32], А.С. Цыганков [33], Д.В. Ушаков [34] и Д.С. Лаврова [35]; по применению интеллектуальных подходов к управлению ИБ — И.В. Машкина [36], Р.А. Демидов [37] и Г.В. Карайчев [38]. Центры мониторинга ИБ (*SOC*) первого поколения упоминаются всего в двух работах: И.А. Шелудько («Разработка и исследование системы оперативного сетевого мониторинга событий безопасности») (2004 г.) [39] и Д.О. Ковалева («Выявление нарушений информационной безопасности по данным мониторинга информационно-телекоммуникационных сетей») (2011 г.) [40]. Проведенный анализ показал, что в настоящее время проблема обеспечение ИБ ИТКС с применением современных интеллектуальных подходов до сих пор остаётся до конца научно не решенной, а обеспечение ИБ ИТКС на основе создания специализированного структурного элемента в составе ИТКС ранее не было темой специального комплексного научного исследования.

Цель исследования: разработка научно обоснованной методологии и принципов построения специализированного структурного элемента ИТКС — типового ЦИУСБ в составе СОИБ ИТКС, призванного осуществлять упреждающее управление сетевой безопасностью при передаче данных в ИТКС на всех стадиях ее жизненного цикла за счет прогнозирования развития событий в области ИБ ИТКС и применения в ЦИУСБ для достижений этих целей интеллектуальных подходов обработки больших относящихся к ИБ ИТКС данных. При этом все процессы обеспечения ИБ с применением ЦИУСБ в ИТКС организации будут работать наиболее результативно только в том случае, когда операционные (текущие), тактические (в ближайшей перспективе) и стратегические (в отдаленной перспективе) задачи обеспечения ИБ ИТКС будут четко определены и будут решаться на взаимоподдерживающей основе в рамках СОИБ ИТКС.

Для реализации цели были поставлены и решены *следующие задачи исследования*:

1. Обосновать включение в ИТКС как основного объекта защиты в ЕИП организации (объектов КИИ) нового специализированного структурного элемента, предназначенного для упреждающего управления сетевой безопасностью ИТКС на всех стадиях ее жизненного цикла, выявив противоречие между усложнившимся характером современных сетевых атак и существующими подходами и средствами обеспечения сетевой безопасности.

2. Провести научно обоснованную структуризацию понятий информационной защищенности ИТКС и описания внутреннего и внешнего контекста деятельности организации в виде единой таксономии, необходимой для конкретизации требований к ЦИУСБ, которая позволит получить научную систематизацию и совокупность классификаций сложноорганизованных иерархически взаимосвязанных сущностей (базовых понятий ИБ: «уязвимость», «угроза ИБ», «сетевая атака» и «инцидент ИБ»).

3. Исследовать основные подходы к управлению сетевой безопасностью и разработать и формализовать процесс управления инцидентами ИБ (ПУИИБ) для его реализации в ЦИУСБ как ключевой структуры системы управления инцидентами ИБ ИТКС, а следовательно, и СОИБ ИТКС.

4. На основе анализа недостатков известных видов центров управления безопасностью обосновать применимость концепции интеллектуальной безопасности с расширенной бизнес-логикой функционирования в разрабатываемом типовом ЦИУСБ, а также сформулировать требования к нему.

5. Разработать и применить научно обоснованную методологию и принципы построения типового ЦИУСБ, включая решение задач разработки функциональной архитектуры, архитектуры обработки относящихся к ИБ данных и архитектуры обеспечения собственной ИБ ЦИУСБ с *SIEM*-системой следующего поколения в качестве его ядра и исследование вопросов обеспечения его функциональной устойчивости в ЕИП организации и кадрового обеспечения.

Методология и методы исследований. В основу исследования положены общая методология построения систем, общая теория систем, теория открытых систем, теория управления, теория связи, передачи, обработки и хранения информации, теория информационно-телекоммуникационных систем и сетей, теория ИБ, а также ИТ больших данных и блокчейна. Применимые к исследованию методы исследования: аналитические подходы, а именно системный анализ объекта исследования, позволяющий провести его высокоуровневое моделирование; поисковые исследования, анализ, систематизация и классификация типичных уязвимостей элементов ИТКС,

угроз ИБ, сетевых атак и инцидентов ИБ; процессный подход, используемый для описания управления ИБ, включая мониторинг ИБ, современных сетей; аналитическое исследование текущего состояния предмета исследования; сравнительный анализ двух поколений ЦУБ и *SIEM*-систем; синтез требований к новой структурной единице ИТКС для осуществления централизованного управления ее ИБ с учетом основных положений теории управления и выявления ближайших аналогов; синтез требований к следующему поколению *SIEM*-систем как ядру ЦИУСБ, методы нечетких множеств, лингвистических переменных (нестрогой математики), неформального оценивания, неформального поиска оптимальных решений; оценка разработанной концепции ЦИУСБ; метод карт процессов для представления процесса управления инцидентами ИБ; разработка глоссария основных понятий, используемых в исследовании.

Структура монографии включают введение, пять глав, заключение, список литературы и разработанный глоссарий.

Во введении обоснована актуальность исследования, определены его объект и предмет, а также сформулированы цель и задачи и перечислены полученные результаты.

В первой главе с целью постановки научной проблемы исследования и определения его границ на основе критического анализа положения дел по исследуемому вопросу и открытых источников выбирается и описывается объект исследования — типовая ИТКС организации, вводятся основы терминологического аппарата, используемого в монографии, а также выделяются особенности текущего состояния обеспечения ИБ информационных ресурсов ИТКС в условиях существования угроз ИБ в ЕИП организации, для чего прослеживается эволюция средств обеспечения сетевой безопасности начиная с 70-х годов XX века и по настоящее время. Выбирается нормативная и правовая база в области обеспечения ИБ, взятая за основу при проведении исследования.

Во второй главе разрабатывается таксономия взаимосвязанных сущностей — базовых понятий ИБ («уязвимость», «угроза ИБ», «сетевая атака» и «инцидент ИБ») для ИТКС, необходимых для упорядочивания знаний об информационной защищенности ИТКС организации и которые следует своевременно предотвращать или устранять, если они уже состоялись и были выявлены. Написание адекватных Стратегии и Политик ИБ, обоснованная разработка системы и выбор методов и средств обеспечения ИБ для ИТКС организации напрямую зависит от полноты и качества разработанной таксономии и представленных классификаций.

В третьей главе для ИТКС организации как основного объекта защиты в ЕИП организации определяются понятия «процесс»,

«результативность процесса», «эффективность процесса», «обеспечение ИБ», «информационная защищенность», «СОИБ», «управление ИБ», «система управления ИБ», «мониторинг ИБ» и другие. На этой основе детально описываются процессы обеспечения и управления ИБ, показывается их взаимная связь и даются определения обеспечения и управления сетевой безопасностью ИТКС организации. Приводятся результаты анализа эволюции основных подходов к управлению сетевой безопасностью. Перечисляются основные процессы проверки ИБ с особым вниманием к процессу мониторинга ИБ ИТКС организации как основы выявления событий, связанных с ее ИБ, в рамках функционирования ЦИУСБ организации. Подробно разрабатывается являющийся основой деятельности ЦИУСБ организации процесс управления инцидентами ИБ для ИТКС с детальным представлением карт его процессов и их описанием. В заключении раздела показывается место разрабатываемого ЦИУСБ среди систем обеспечения и управления ИБ организации в качестве фундамента системы управления инцидентами ИБ ИТКС.

В четвертой главе вводится и подробно анализируется понятие являющейся ядром ЦМБ и ЦИБ *SIEM*-системы как основы для дальнейшего построения ЦИУСБ, устраняющей ограниченность своих предшественников. Поясняется концепция интеллектуальной безопасности (*Security Intelligence*), положенная в основу разрабатываемого ЦИУСБ. Анализируются два вида ЦУБ: ЦМБ, осуществляющего только мониторинг инцидентов ИБ, и ЦИБ, способного управлять инцидентами ИБ в ИТКС. Для ЦИБ разрабатывается расширенная по сравнению с оригинальной бизнес-логика функционирования для ее дальнейшего применения в типовом ЦИУСБ. Рассматриваются различные модели зрелости ЦУБ. Глава завершается формулированием общих и специальных требований, требований по обеспечению собственной ИБ ЦИУСБ.

В начале пятой главы пояснена хронология событий, касающихся идеи автора исследования разработать типовой ЦИУСБ и состояния этого вопроса в отечественной и зарубежной науке. Далее излагается разработанная методология построения типового ЦИУСБ организации, после чего формулируются основные принципы его построения. Представляется основная идея построения и функциональные возможности типового ЦИУСБ как центра, объединяющего все преимущества ЦИБ И СОЦ в одном месте организации для централизованного управления ИБ ИТКС и, в частности, ПУИИБ. Рассмотрены вопросы визуализации информации в типовом ЦИУСБ для принятия решений по управлению инцидентами ИБ в ИТКС. С учетом требований, изложенных в четвертой главе, для типового

ЦИУСБ разрабатываются три основные архитектуры — функциональная, обработки больших и быстрых относящихся к ИБ ИТКС данных и обеспечения собственной ИБ. Кроме этого, для обеспечения ИБ названных данных, поступающих для обработки в *SIEM*-систему ЦИУСБ, представлен проект *SIEM*-системы 3.0 с новым элементом, построенным с применением технологий блокчейна. Завершает главу рассмотрение вопросов функциональной устойчивости ЦИУСБ в штатном режиме и в условиях угроз ИБ в ЕИП организации, кадрового обеспечения ЦИУСБ высококвалифицированными специалистами и демонстрация выполнения в разработанном типовом ЦИУСБ сформулированных в четвертой главе требований.

В заключении выделены основные результаты исследования, а также указаны возможные направления дальнейших исследований.

1 Анализ текущего состояния обеспечения информационной безопасности информационно-телекоммуникационных сетей

В главе с целью постановки научной проблемы исследования и определения его границ на основе критического анализа положения дел по исследуемому вопросу и открытых источников выбирается и описывается объект исследования — типовая информационно-телекоммуникационная сеть (ИТКС) организации, вводятся основы терминологического аппарата, используемого в монографии, а также выделяются особенности текущего состояния обеспечения информационной безопасности (ИБ) информационных ресурсов ИТКС в условиях существования угроз ИБ в едином информационном пространстве (ЕИП) организации, для чего прослеживается эволюция средств обеспечения сетевой безопасности начиная с 70–х годов XX века и по настоящее время. Выбирается нормативная и правовая база в области обеспечения ИБ, взятая за основу при проведении исследования. В заключении главы формулируются цель и задачи исследования.

1.1. Анализ информационно-телекоммуникационной сети как основного объекта защиты в едином информационном пространстве организаций

1.1.1. Особенности современного использования информационно-телекоммуникационных сетей

Современные организации разных размеров, сфер деятельности и типов (государственные учреждения, коммерческие компании, некоммерческие организации) и их работники используют различные сетевые технологии для повседневной деятельности, корпоративного обучения, организации деловых мероприятий, взаимодействия с бизнес-партнерами и т. д., что предполагает активный обмен информацией в глобальном масштабе с помощью предоставляемых дистанционно услуг, безопасность которых не гарантирована и не доказана. Деятельность этих организаций базируется на гетерогенных распределенных сетевых инфраструктурах, предлагающих потребителям различные информационные ресурсы и услуги. Подключение к компьютерным сетям может осуществляться из любо-

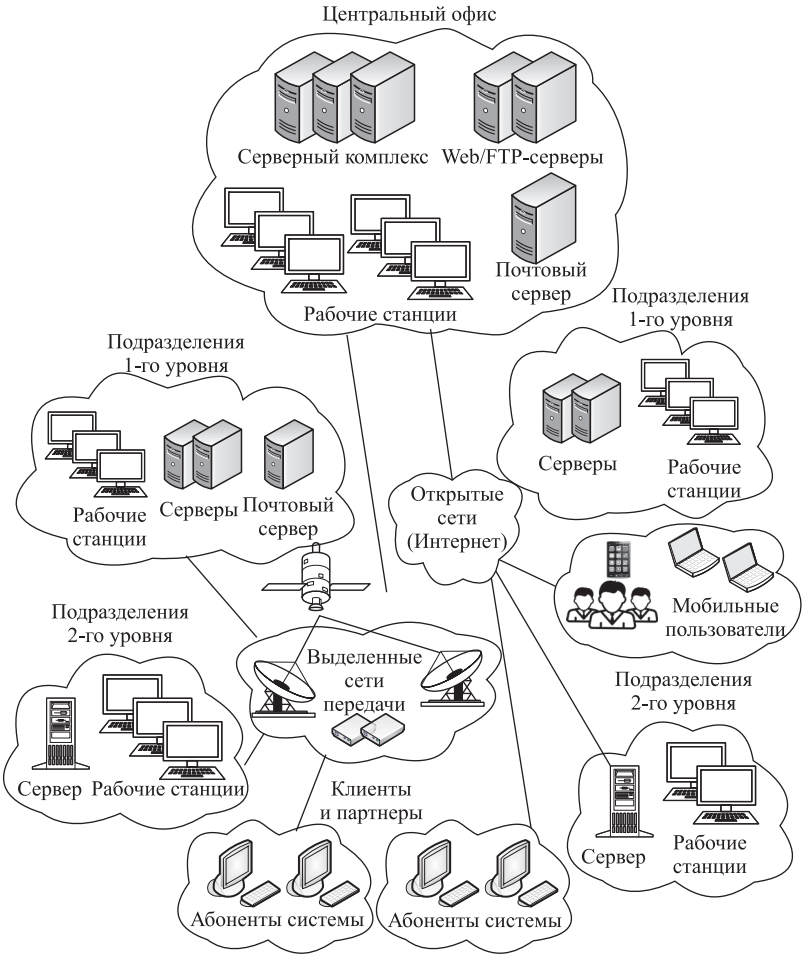

Рис. 1. Типовая схема распределенной сети организации

го места планеты в любое время. Облачные технологии, инструменты виртуализации, мобильные (беспроводные) сети, домашние офисы, роуминг, многочисленные персональные устройства и т. п. стали обычной реальностью, размывающей периметр сетей организаций. Локальные (автономные) компьютеры практически ушли в прошлое, что означает, что любая сеть начинается или заканчивается на любом подключенном к ней устройстве. Для различных групп пользователей требуется бесперебойная работа и дифференцированное качество обслуживания. Широкое распространение теневых сетей (типа *Tor*, *DarkNet*) и средств работы в них добавляет негативных красок в эту картину. При этом ценность коммерчес-

кой информации, персональных данных, платежной информации и т. п. возрастает день ото дня — давно стало истиной то, что те, кто владеет информацией, владеют миром. Также растет количество вовремя не устраненных уязвимостей в веб-технологиях, программном (ПО) и аппаратном (АО) обеспечении. Неверно настроенные системы защиты, отсутствие необходимых политик, руководств и регламентов в области обеспечения информационной безопасности, избыточные права доступа — далеко не все типичные проблемы, используемые злоумышленниками для реализации как простейших, так и сложных и разрушительных целенаправленных атак на информационные системы (ИС), подключенные к сетям. Кроме того для достижения своих бизнес-целей и поддержания конкурентоспособности, защиты клиентов и сотрудников не только внутри, но и вне самой организации, для нее важно соответствовать множеству внутренних и внешних требований.

Типовая схема распределенной корпоративной компьютерной сети (интранета), обеспечивающей разным группам пользователей ее использование и совместный доступ к услугам, процессам и информационным ресурсам, находящимся в разных подразделениях, упрощенно представлена на рис. 1 [55]. Она отличается существенной неоднородностью используемых в разных подразделениях АО и ПО и интеграцией этих гетерогенных компонентов в единую систему, различными технологиями подключения потребителей предоставляемых услуг к общей сети, необходимостью дифференцированного качества обслуживания отдельных групп пользователей и всеми ранее перечисленными особенностями.

Представленное поверхностное описание создает далеко не полное представление о современном мире компьютерных сетей и насущной потребности организаций в защите их информационных ресурсов и предоставляемых пользователям услуг.

1.1.2. Определение информационно-телекоммуникационной сети

Согласно Федеральному закону № 187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации», информационно-телекоммуникационные сети, ИС, автоматизированные системы управления (АСУ) субъектов критической информационной инфраструктуры (КИИ), а также сети электросвязи, используемые для организации взаимодействия таких объектов, относятся к объектам КИИ. Под субъектами КИИ подразумеваются государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели (далее — организация), которым на праве собствен-

ности, аренды или на ином законном основании принадлежат ИС, ИТКС, АСУ, функционирующие в сфере здравоохранения, транспорта, связи, энергетики, науки, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей [7, статья 2].

Как определяется в Федеральном законе № 149-ФЗ «Об информации, информационных технологиях и о защите информации», *информационно-телекоммуникационная сеть* — это технологическая система (ТС), предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники (СВТ) [6, статья 2]. В свою очередь, ТС — это совокупность функционально взаимосвязанных средств технологического оснащения, предметов производства и исполнителей для выполнения в регламентированных условиях производства заданных технологических процессов или операций. Выделяют четыре иерархических уровня таких систем: операций, процессов, производственных подразделений и предприятий [56]. СВТ — это совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем [57].

Самым полным и детальным с точки зрения автора исследования описанием информационно-телекоммуникационной системы (ИТС), включающей в свою архитектуру ИТКС, является описание, данное М.Ю. Сенаторовым для ИТС Банка России [58]. Поэтому именно оно и было взято за основу формирования общесистемного представления о типовой ИТКС организации.

Современные ИТКС могут быть глобальными (типа Интернета), локальными (в одном здании организации), корпоративными (для одной корпорации), региональными (в пределах городов, областей и других территориальных единиц), ведомственными (в пределах ведомства) и специального назначения (например, ГАС «Выборы»). При этом ИС большинства государственных учреждений и коммерческих компаний, организующие хранение и обработку информации о конкретной предметной области [59], связаны между собой компьютерными сетями. Их сетевые соединения могут существовать в пределах одной организации (организации А и В), между различными организациями (организации А и С) или между организацией и неограниченным кругом лиц (организации А и С) (рис. 2) [60].

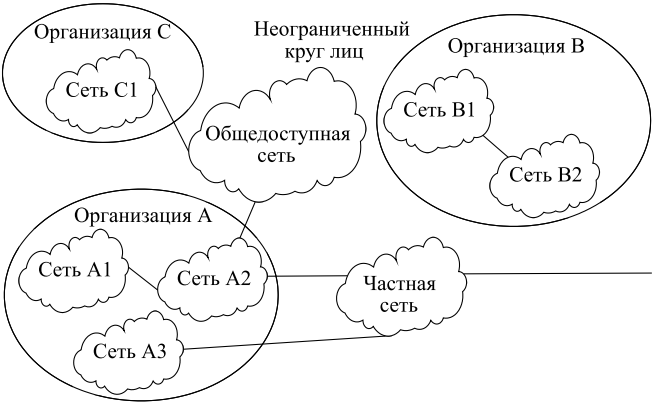

Рис. 2. Виды сетевых соединений

1.1.3. Информационно-телекоммуникационная сеть как симбиоз телекоммуникационной и информационной сетей

Как следует из названия, ИТКС представляет собой симбиоз двух видов сетей — информационной и телекоммуникационной [61]. Эти сети территориально распределены по месту размещения, объединяют большое количество разнообразных технических средств обработки, передачи и хранения информации, различаются по масштабу, решаемым задачам и типам обрабатываемых данных с разными требованиями по обеспечению ИБ, а также реализуют сложные режимы автоматизированной обработки данных и совмещают выполнение информационных запросов различных категорий пользователей — потребителей информации и ИТ-услуг (услуг информационных технологий (ИТ), *IT services*). При этом все составляющие ИТКС должны функционировать непрерывно и устойчиво в условиях высокой интенсивности информационных потоков.

Телекоммуникационная сеть является системообразующим компонентом в общей архитектуре организации, выполняя роль интегратора при перемещении информационных ресурсов, и представляет из себя совокупность взаимосвязанного телекоммуникационного оборудования — технических средств (устройств, оборудования), используемых для построения сетей передачи данных и приема-передачи цифровой информации и предоставления телекоммуникационных услуг конечным потребителям (адаптировано на основе [62, 63]). Цифровая информация (*digital information*) — это информация, представленная в виде последовательности цифр и доступная для обработки, передачи и хранения с помощью технических устройств в результате применения ИТ. К телекоммуникационным