ВВЕДЕНИЕ

Эффективность работы корпоративных сетей в современном мире во многом зависит от уровня обеспечения их информационной безопасности [1–3]. В настоящее время для достижения необходимой и достаточной защищенности организации и ее корпоративных сетей необходимо решать большой спектр задач, таких как противодействие деструктивному контенту [4–9] и другим эпидемическим вредоносным процессам [10–15], особенно в борьбе с сетевыми атаками [16–18].

Так, с октября по декабрь 2022 года было зафиксировано 281 тыс. событий безопасности, что на треть превышает аналогичный показатель III квартала 2021 года (214 тыс. инцидентов), и это самый высокий квартальный показатель за весь 2022 год [16]. Рассмотрев более детально информацию о появляющихся инцидентах, можно отметить следующее: вредоносное программное обеспечение (ВПО) все еще является главным инструментом злоумышленников. Однако в III квартале был замечен рост фишинг-атак с вредоносным содержимым, но к концу IV квартала атаки стали уменьшаться. Это свидетельствует о том, что организациями активнее ведется борьба с ВПО и они повышают осведомленность своих сотрудников в вопросах сетевой безопасности.

Новые данные компании «Ростелеком-Солар» за I квартал 2023 год показывают, что было зафиксировано 290 тыс. событий безопасности [17]. Если сравнивать с IV кварталом предыдущего года, то число сетевых атак выросло на 3 %. Злоумышленники по-прежнему используют те же вектора атак, но только более тщательно готовятся, ведя активную сетевую разведку для того, чтобы выявить уязвимые места в системе.

Ключевым моментом реализации сетевых атак являются обилие незащищенных уязвимостей, которые используют злоумышленники в своих атаках. Данная проблема ярко отража-

ется в отчетах отдела анализа защищенности центра противодействия кибератакам Solar JSOC за период с марта 2022 года по март 2023 года [18], при этом в исследовании принимало участи около 80 организаций. Его результаты показали недостаточный уровень защищенности корпоративных сетей: в 93 % случаях присутствуют незакрытые уязвимости, посредством которых злоумышленник легко может реализовать атаку. Поэтому значительную роль в борьбе с сетевыми атаками играют не только знания техник их реализации, но и осведомленность относительно уязвимостей корпоративной сети организации (далее Организация), эксплуатируемых этими векторами атак.

Вышеизложенное свидетельствует о том, что арсенал противодействия сетевым атакам все еще не совершенен, в том числе в части организационно-правовой защиты Организаций, разрабатывающих политики, регламенты и инструкции как основной вид документов обеспечения информационной безопасности их корпоративных сетей.

Следуя этой триаде внутренних документов, Организация может гарантировать защиту своим сотрудникам, имуществу, информации, деловой репутации и бизнес-процессам от возможных угроз нарушения безопасности, что соответствует лучшим практикам и международным стандартам и является необходимым требованием конкурентоспособности в современном мире. При этом руководство Организации должно осознавать, что продвижение и совершенствование мер по обеспечению информационной безопасности являются важными и необходимыми условиями в контексте развития защиты своих активов. При соблюдении принципов информационной безопасности Организация может укрепить свои конкурентные преимущества, соответствовать правовым, регуляторным требованиям, а также минимизировать имиджевые риски.

Проанализировав основные рекомендации по созданию организационно-правовой документации [19–23], можно выделить главную проблему, состоящую в том, что в основном в ней (документации) приводятся общие шаблоны по формированию защитных мер и нигде не учитывается специфика защиты от сетевых атак конкретного типа.

Для решения возникающей проблемы можно воспользоваться аппаратом анализа и управления рисками, который позволит идентифицировать наиболее опасные сочетания векторов атак и уязвимостей, оценить масштаб их воздействия на Организацию и

в дальнейшем предложить меры ее защиты в виде разработанной организационно-правовой документации [24–29].

В настоящее время активно ведутся исследования по противодействию различным атакам на основе риск-анализа [30–36]. Применение такого подхода к анализу и управлению рисками возникло сравнительно недавно. Управление рисками строится на международных стандартах ISO IEC 17799, ISO IEC 27001, британском стандарте BS 7799-3, американском стандарте NIST 800-30 и отечественных нормативно-правовых документах [71–76]. На их основе представляется возможным предложить концептуально новый подход к проведению риск-анализа как инструмента совершенствования организационно-правового противодействия сетевым атакам.

Основная задача риск-анализа будет заключается в сборе данных и знаний о сетевой атаке. Интернет-статистика позволяет на основе оценки риска выявить наиболее опасные сочетания векторов атаки и уязвимостей. Затем с помощью информационного обеспечения, полученного на первом этапе исследования, можно отыскать взаимно однозначное соответствие между проанализированными аспектами заданного типа атак и брешами в организационно-правовых режимах традиционной конфигурации, сохраняющих популярность рассматриваемого класса атак в деструктивном воздействии на корпоративные сети [77–120]. Собственно этому и посвящена первая глава монографии.

Особое значение имеет сетевая разведка, которая является неотъемлемой и вступительной частью практически всякой кибератаки, ибо подготавливает всякое несанкционированное проникновение в корпоративную сеть [121]. Она позволяет получить необходимую злоумышленнику информацию о топологии сети, технических характеристиках серверов, автоматизированных рабочих мест, сетевого оборудования, а также об их уязвимостях и способах защиты атакуемой сети. Процесс получения и анализа информации о технической инфраструктуре и системах безопасности Организации осуществляется с целью предварительной подготовки целенаправленной атаки. Проблема обнаружения признаков сетевой разведки сопоставима с задачей обнаружения аномалий в сетевом трафике, поскольку в обоих случаях возникает значительное количество подозрительного трафика на сетевом и транспортном уровнях. Следовательно, аномальные признаки сетевого трафика могут свидетельствовать о разведывательных действиях со стороны злоумышленника [122].

Сетевая разведка используется не только спецслужбами, но и частными компаниями, чтобы получать конкурентные преимущества в собственной деятельности организации. Согласно отчету Positive Technologies (10 февраля 2023 г.) более чем в трети компаний (38 %) в ходе пилотных проектов были зафиксированы случаи сетевой разведки [123].

В условиях сетевого противоборства, помимо технических методов защиты информационного пространства, возникает необходимость в его организационно-правовом регулировании. На уровне Организации это можно реализовать с помощью корректно разработанных частных политик, регламентов, инструкций обеспечения информационной безопасности, опирающиеся на риск-анализ атаки [124–127].

По-прежнему актуальна эта проблема ввиду пренебрежения качеством организационно-правого обеспечения в отечественных организациях. Данный феномен связан с тем, что в российском законодательстве нет единого стандарта для составления частных политик и вытекающих из нее регламентов и инструкций. В связи с чем существует тенденция «слепого» копирования частных политик, имеющихся в общедоступных источниках. Документы, разработанные таким способом, несут существенные информационные риски для Организации и ее сотрудников [128]. Отсюда цель исследования [48–65] заключается в повышении защищенности корпоративных сетей за счёт формирования (посредством риск-анализа) методологии сетевой контрразведки путём создания комплекса мер и средств организационно-правового направления, обеспечивающих снижение рисков успешности атаки типа «сетевая разведка».

Для достижения поставленной цели необходимо решить следующие задачи: на основании статистики частоты и ущербности атак сетевой разведки выявить наиболее опасные сочетания сценариев и уязвимостей, с которыми может столкнуться компания при обеспечении своей информационной безопасности; для выявленных наиболее опасных сочетаний сценариев и уязвимостей предложить частную политику, регламенты и инструкции по защите корпоративной сети от сетевой разведки. Этому посвящена вторая глава монографии.

Ожесточенность межсетевого противоборства красноречиво свидетельствует о том, что мир тесен и потому весьма опасен. Его мультисетевая организация сегодня ежедневно увеличивает эту тесноту и риски нарушения безопасности ее пользователей

[10, 41–45]. При этом масштабные и всесторонние исследования методов и средств защиты информации [187–199], увы, не позволяют никакой системе считать себя абсолютно защищенной.

В этом контексте появились киберполигоны [187–195], позволяющие виртуально моделировать процессы информационного противоборства, эмулировать атаки и настраивать противовредоносные компоненты тестируемых объектов. Актуальность таких систем не вызывает у проектировщиков сомнений. Однако совершенными их назвать нельзя. Поэтому в третьей главе монографии объектом исследования избраны киберполигонные решения учебного и научно-технического профиля, а предметом исследования стали концепции, архитектура и функциональные возможности киберполигонных построений, отвечающие требованиям современности.

Все вышеперечисленное позволяет сформулировать цель исследования — повышение защищенности тестируемых в киберполигоне систем и сетей за счет формирования его социотехнической архитектуры, внедрения организационно-правовых норм развития полигонного хозяйства, формализации целеполагания его проектной деятельности, отработки методик на примерах обеспечения полигонных киберучений.

Для достижения сформулированной цели необходимо решить следующие задачи:

- построение архитектуры и обеспечение комплексного социотехнического подхода в создании киберполигона, учитывающих не только технический, но и человеческий факторы информационного противоборства;
- формирование организационно-правового обеспечения реализации программы «Киберполигон» с учетом творческого потенциала и опыта кафедры в решении задач обеспечения информационной безопасности;
- формализация целеполагания проектной деятельности в оценке и регулирования рисков нарушения безопасности систем и сетей, создаваемых и тестируемых в киберполигоне;
- создание (для примера) методического и программного обеспечения для проведения полигонных киберучений моделирования эпидемических процессов в сетевых структурах с произвольной топологией.

Решению вышеперечисленных задач посвящена третья глава работы.

В целом монография ориентирована на оценку состояния и перспективы совершенствования обеспечения безопасности информационных сетей при реализации атак различных типов, включая формирование частных политик, регламентов и инструкций, организационно сетевой разведки, а также освоение и обработку техник противоборства в рамках корпоративного киберполигона.

Авторы выражают благодарность Д.С. Печкину за помощь в оформлении рукописи настоящей монографии.