DOI 10.36622/VSTU.2023.26.3.023
УДК 004.056

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ АСПЕКТЫ ЗАЩИТЫ КОРПОРАТИВНЫХ СЕТЕЙ: НАУЧНО-ПРАКТИЧЕСКИЕ РЕАЛИИ И ГОРИЗОНТЫ

Д.В. Щербакова

В работе рассматриваются вопросы защиты корпоративных сетей. В этой связи осуществлено целеполагание данного исследования с акцентом на организационно-правовые аспекты. Предлагается методическое обеспечение борьбы с сетевыми вторжениями через риск-формализацию деятельности корпоративных сетей в части формирования адекватных атакам политик, регламентов и инструкций защищаемых организаций. Особое внимание уделяется формированию сетевой контрразведки, ибо все современные атаки предварительно готовятся на основе данных, полученных в ходе реализации сетевых разведывательных действий. В этой связи предлагаются формы соответствующей регламентации. Рассматриваются концепция, функционал и архитектура корпоративного полигона как тренажера персонала организации в ходе сетевого противоборства.

Ключевые слова: безопасность, корпоративная сеть, политика безопасности, регламент безопасности, инструкции безопасности, сетевая контрразведка, киберполигон.

Введение

Сегодня эффективность работы корпоративных сетей во многом зависит от уровня обеспечения их информационной безопасности [1-3]. Сейчас для достижения необходимой и достаточной защищенности организации и ее корпоративных сетей, необходимо решать большой спектр задач, особенно в борьбе с сетевыми атаками [4-8]. Только с октября по декабрь 2022 года было зафиксирована 281 тысяча 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 [1]. При этом, можно утверждать, что вредоносное программное обеспечение (ВПО) все еще является главным инструментом злоумышленников. В III квартале 2022 года был замечен рост фишинг-атак с вредоносным содержимым, но к концу IV квартала количество таких атак стало уменьшаться. Это свидетельствует о том, что организациями активнее ведется борьба с ВПО, и они повышают осведомленность своих сотрудников в вопросах сетевой безопасности.

Данные компании «Ростелеком-Солар» за I квартал 2023 год показывают, что было зафиксировано 290 тыс. событий безопасности [2]. 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.

Успеху реализации сетевых атак способствует обилие незащищенных уязвимостей, которые используют злоумышленники в своих атаках. Данная проблема ярко отражается в отчетах отдела анализа защищенности центра противодействия кибератакам Solar JSOC за период с марта 2022 года по март 2023 года [3], где в исследовании принимало участи порядка 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).

Целеполагание исследования

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.

В отношении создания организационно-правовой документации [4-8], можно выделить главную проблему, состоящую в том, что в основном в ней приводятся общие шаблоны по формированию защитных мер и нигде не учитывается специфика защиты от сетевых атак конкретного типа.

Для разрешения этой 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 [4-8].

В настоящее время ведутся активно исследования по противодействию различным атакам на основе риск-анализа. 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. 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.

Особое значение имеет сетевая разведка, которая является неотъемлемой и вступительной частью практически всякой кибератаки, ибо подготавливает несанкционированное проникновение в корпоративную сеть. 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.

Используется сетевая разведка 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.

Помимо технических методов защиты информационного пространства, в условиях сетевого противоборства возникает необходимость в его организационно-правовом регулировании. На уровне организации это возможно реализовать с помощью корректно разработанных частных политик, регламентов, инструкций обеспечения информационной безопасности, опирающихся на риск-анализ атаки.

Обычно эта проблема актуальна, 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 их 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. Отсюда цель исследования заключается в повышение 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.

Ожесточенность сетевого противоборства красноречиво свидетельствует о том, что мир тесен и потому весьма опасен. Его мультисетевая организация сегодня ежедневно увеличивает эту тесноту и риски нарушения. При этом даже всесторонние исследования методов и средств защиты информации, увы, не позволяют никакой системе считать себя абсолютно защищенной.

В этом контексте появились киберполигоны, позволяющие виртуально моделировать процессы информационного противоборства, эмулировать атаки и настраивать антивредоносные компоненты тестируемых объектов. Актуальность таких систем не вызывает у проектировщиков сомнений. Однако совершенными их назвать нельзя. Поэтому объектом исследования должны быть киберполигонные решения учебного и научно-технического профиля, а предметом исследования станут концепция, архитектура и функциональные возможности киберполигонных построений, отвечающие требованиям современности.

Все вышеперечисленное позволяет сформулировать цель исследования в качестве: повышения 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 решать 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.

В целом, следует сориентироваться на состояние и перспективу совершенствования обеспечения безопасности информационных сетей при реализации атак различных типов, включая: формирование частных политик, регламентов и инструкций; организацию сетевой контрразведки; а также освоение и обработку техник противоборства в рамках корпоративного киберполигона.

Первичные результаты исследования

Исходя из вышеприведенного целеполагания, были проведены исследования, где осуществляется формализация описания процесса информационного противоборства, на основе соответствия между векторами (сценариями) сетевых атак и уязвимостями, для которого предложено методическое обеспечение построения риск-ландшафта атакуемой корпоративной сети. методики оценки риска позволяют определить наиболее опасные сочетания вектора атаки и уязвимости, чтобы в дальнейшем предложить для них меры защиты на организационно-правовом уровне. На основании действующих нормативно-правовых документов, учитывая риск-ландшафт, предложена методика построения частной политики сетевой безопасности, которая сформирована в виде документа, содержащего окна, которые необходимо адаптировать под конкретную атаку. В соответствие с целями частной политикой разработаны частные регламенты сетевой безопасности по следующим направлениям: регламент обнаружения и регистрации инцидентов нарушения безопасности, регламент реагирования на инциденты нарушения безопасности, регламент ликвидации последствий инцидентов нарушения безопасности (табл. 1-4). Кроме того, предложены методики построения частных инструкций сетевой безопасности для администратора безопасности, внутренних и внешних пользователей в контексте противоборства различным сетевым атакам.

Таблица 1

Оперативный отчет по обнаружению инцидентов нарушения безопасности в организации

Дата и время	Тип инцидента	Критическое значение инцидента	Затронутые контролируемые инциденты	Имя пораженной подсистемы ИР	Прикладной сервис ИР	Имя субъекта
ДД.ММ.ГГГГ ЧЧ:ММ	*Классификация инцидента ИБ*	*Критичность инцидента*	*Классификация информационных ресурсов*	*Имя (IP-адрес)*	*Название сервиса (если применимо)*	*ФИО, имя учетной записи*
Краткое описание инцидента ИБ: 1. Место, дата и время возникновения инцидента нарушения безопасности: _____ 2. Из какого источника была получена информация об инциденте нарушения безопасности: _____ 3. Возможные причины возникновения инцидента нарушения безопасности: _____ 4. Описание инцидента нарушения безопасности и его последствий (если возможно установить на текущем этапе): _____						

Таблица 2

Карточка регистрации инцидента

<table>
<tr><td colspan="3">Номер инцидента</td><td colspan="3">010-6661</td></tr>
<tr><td colspan="3">Дата и время получения информации об инциденте</td><td colspan="3">01.01.2001 00:01</td></tr>
<tr><td colspan="3">Источник информации об инциденте, канал получения информации</td><td colspan="3">Сообщение по телефону от сотрудника отдела кадров Сидорова И.И.</td></tr>
<tr><td colspan="3">Идентификаторы информационных ресурсов, затронутых инцидентом ИБ;</td><td colspan="3">R_1</td></tr>
<tr><td colspan="3">Инвентаризационная информация об информационных ресурсах, затронутых инцидентом ИБ</td><td colspan="3">Ресурс R_1относится к отделу №1, находиться в каб.001 и представляет собой СУБД из состава АРМ№1</td></tr>
<tr><td>Описание инцидента</td><td colspan="5">Со слов Сидорова И.И. 01.01.2001 в 00:01им к своему АРМ был подключен внешний носитель информации (флэш-карта) с данными необходимыми для выполнения должностных обязанностей. После прохождения антивирусной проверки Сидоров И.И. получил доступ к данным на флэш-карте. После запуска файла формата *.docx работа АРМ Сидорова И.И. заметно замедлилась и Сидоров И.И. принял решение перезагрузить АРМ нажав «Пуск-Выключение-Перезагрузка». После выключения ОС АРМ не загрузилась, и Сидоров сообщил о произошедшем.</td></tr>
<tr><td>Тип инцидента</td><td>Уровень ИТ-инфраструктуры</td><td>Нарушенные свойства информации</td><td>Преднамеренность</td><td>Тяжесть инцидента</td><td>Описание инцидента</td></tr>
<tr><td>Отказ в обслуживании</td><td>Операционной системы</td><td>Целостность Доступностью</td><td>Непреднамеренный (предварительно)</td><td>Легкая</td><td>Заражение вредоносным ПО (предварительно)</td></tr>
<tr><td colspan="3">Действия по регулированию инцидента</td><td colspan="3">В рамках Регламента реагирования на инциденты безопасности</td></tr>
</table>

Таблица 3

Отчет о реагировании на инцидент нарушения безопасности

№	Данные об инциденте	Описание параметра
Сведения об инциденте		
1	Идентификатор инцидента	*Например: I_1*
2	Дата и время начала инцидента	*ДД.ММ.ГГГГ ЧЧ:ММ*
3	Дата и время обнаружения инцидента	*ДД.ММ.ГГГГ ЧЧ:ММ*
4	Дата и время оповещения об инциденте	*ДД.ММ.ГГГГ ЧЧ:ММ*
Критичности инцидента		
1	Значение критичности инцидента	*Например: высокий*
2	Приоритет инцидента	*Например: средний*
Сведения о мерах по реагированию на инцидент		
Состав рабочей группы реагирования на инцидент		
1	Начальник отдела защиты информации	*Указываются ФИО*
2	Администратор информационной безопасности	*Указываются ФИО*
3	Системный администратор	*Указываются ФИО*

Продолжение табл. 3

№	Данные об инциденте	Описание параметра
Запланированные мероприятия по локализации инцидента		
1	Описание задачи	*Указываются действия, направленные на локализацию инцидента*
2	Фамилия, имя, отчество участника рабочей группы реагирования, ответственного за выполнение задачи	*Пример заполнения: Сидоров Иван Петрович*
3	Срок выполнения задачи	*ДД.ММ.ГГГГ ЧЧ:ММ*
4	Отклонение по срокам	*В отчете указывается количество дней или часов, в течение которых были зафиксированы отклонения, либо отмечается, что отклонений не было обнаружено.*
5	Основание отклонений	
Сведения о статусе обработки инцидента		
1	Дата и время начала реагирования на инцидент	*ДД.ММ.ГГГГ ЧЧ:ММ*
2	Дата и время локализации инцидента	*ДД.ММ.ГГГГ ЧЧ:ММ*
3	Инцидент полностью устранен	*Да/Нет*
4	Инцидент ИБ невозможно устранить	*Да/Нет*
5	Причины невозможности устранения инцидента	*Указывается причина почему инцидент не удалось устранить*

Таблица 4

Карточка закрытого инцидента нарушения безопасности

№	Собираемые данные об инциденте	Описание значений собранных данных об инциденте
Информация об инциденте		
1	Идентификатор инцидента	*Например:* I_1
2	Краткое описание инцидента	*Приводится краткое описание инцидента и связанных с ним обстоятельств*
3	Описание последствий инцидента	*Приводится описание последствий, масштаба, опасности и критичности инцидента ИБ*
4	Место возникновения инцидента	*Идентификатор контролируемого информационного ресурса и место его размещения*
5	Хронология событий	*Приводится последовательность цепочки событий, которые привели к инциденту*
6	Мероприятия по реагированию на инцидент	*Приводится краткое описание мер по нивелированию инцидента*
7	Меры по ликвидации последствий инцидента	*Приводятся меры по ликвидации последствий инцидента*
Оценка действий ответственных лиц по обнаружению и регистрации инцидента		
1	Время от начала возникновения до момента его регистрации	*ЧЧ:ММ*
2	Время от момента регистрации инцидента до момента его регулирования	*ЧЧ:ММ*
Информация, выявленная в ходе анализа инцидента		
1	Источник инцидента	*Приводится источник инцидента*
2	Краткие сведения об источнике инцидента	*Приводится краткое описание источника инцидента*

Продолжение табл. 4

№	Собираемые данные об инциденте	Описание значений собранных данных об инциденте
Информация, выявленная в ходе анализа инцидента		
3	Действительная или предполагаемая мотивация нарушителя	*Приводится краткое описание модели нарушителя*
4	Факторы, условия или события, которые предшествовали возникновению инцидента	*Приводится описание факторов, условий или событий, которые предшествовали возникновению инцидента*
5	Описание причины возникновения инцидента	*Приводится краткое описание причин возникновения инцидента*
6	Выявленные виновные лица	*Приводится ФИО, должности виновных лиц*
Заключение		
1	Меры, принятые для устранения повторного возникновения инцидента	*Приводятся меры по предотвращению повторного возникновения инцидента*
2	Рекомендации по внедрению новых или изменению имеющихся средств и мер защиты	*Приводятся рекомендации по внедрению новых или изменению (переконфигурированию) применяемых средств обработки и защиты информации и организационных мер*
3	Предложения по совершенствованию подсистем обеспечения ИБ	*Приводится перечень дополнительных средств защиты информации, направленных на повышение уровня защищённости информационных ресурсов*

Результатами исследования являются: риск-ландшафт для наиболее опасных сочетаний сценариев и уязвимостей сетевой разведки; методики формирования частных политик, регламентов и инструкций сетевой контрразведки. Перспективным направлением настоящего исследования станет создание «Библиотеки организационно-правовых рекомендаций по защите корпоративных сетей», для которой разработан формат, систематизированный по типам сетевых атак (табл. 5-9), где в качестве интеллектуальной поддержки специалистов по защите информации в перспективе будут табулированы актуальные меры и средства противодействия злоумышленникам при создании и эксплуатации атакуемых сетей.

Таблица 5

Таблица соответствия действий злоумышленника и мер противодействия им в рамках частной политики обеспечения безопасности при реализации *сетевой атаки типа «..»*

Последовательность и содержание действий злоумышленника в целях реализации *сценариев атаки типа «…»*	Меры защиты организации от сетевой атаки типа «…», адекватные действиям злоумышленника по каждому сценарию
Полное наименование рассматриваемого вектора атаки VA_1	
1.1 …	1.1 …
1.2 …	1.2 …
…	…
Полное наименование рассматриваемого вектора атаки VA_2	
2.1 …	2.1 …
2.2 …	2.2 …
…	…

Таблица 6

Таблица соответствия действий злоумышленника и мер регламентации защиты сети организации на стадии «Обнаружения и регистрации инцидентов безопасности при реализации *сетевой атаки типа «..»*

Типы инцидентов, которые могут возникнуть при реализации действий злоумышленника в ходе сетевой *атаки типа «…»*	Описание инцидента	Средства для обнаружения заданного типа инцидента
Полное наименование рассматриваемого вектора атаки VA_1		
…	…	…
…	…	…
Полное наименование рассматриваемого вектора атаки VA_2		
…	…	…
…	…	…

Таблица 7

Таблица соответствия действий злоумышленника и мер регламентации защиты сети организации на стадии «Реагирование на инциденты безопасности при реализации *сетевой атаки типа «..»*

Произошедшие инциденты в ходе действий злоумышленника в целях реализации *сценариев атаки типа «…»*	Первоочередные меры по предотвращению инцидента	Негативные последствия, вызванные инцидентом безопасности
Полное наименование рассматриваемого вектора атаки VA_1		
…	…	…
…	…	…
Полное наименование рассматриваемого вектора атаки VA_2		
…	…	…
…	…	…

Таблица 8

Таблица соответствия действий злоумышленника и мер регламентации защиты сети организации на стадии «Ликвидация последствий инцидента безопасности при реализации *сетевой атаки типа «..»*

Негативные последствия, вызванные инцидентом безопасности	Меры по устранению инцидента
Полное наименование рассматриваемого вектора атаки VA_1	
…	…
…	…
Полное наименование рассматриваемого вектора атаки VA_2	
…	…
…	…

Таблица 9

Таблица соответствия требования к защите информации от *сетевой атаки типа «..»* и средств защиты информации, обеспечивающие выполнение данных требований

Требование к защите информации от *сетевой атаки типа «..»*	Средство защиты информации, обеспечивающие выполнение данных требований	Рекомендация по настройке параметров средств защиты информации
Полное наименование рассматриваемого вектора атаки VA_1		
…	…	…
…	…	…
Полное наименование рассматриваемого вектора атаки VA_2		
…	…	…
…	…	…

Наконец, были предложены архитектура и функционал корпоративного киберполигона, включающего блоки: актуализации данных и знаний об уязвимостях, векторах и ущербах атак, реализуемых в отношении информационных систем и сетей; эмуляции и риск-анализа кибератак в виртуальном моделировании процесса информационного противоборства; риск-анализ персонала тестируемого объекта на предмет возможного девиантного поведения, порождающего кибер-ущербы; интеллектуальной поддержки программно-технической и организационно-правовой защиты исследуемой кибер-системы. Впервые концепт, архитектура и функционал киберполигона ориентированы на комплексное социотехническое рассмотрение проблем обеспечения информационной безопасности создаваемых и исследуемых в рамках полигона систем и сетей в сочетании с особенностью обслуживающего их персонала. Концепт, архитектура и функционал предлагаемого киберполигона позволяют комплексно анализировать информационную систему или сеть как симбиоз программно-технических решений и персонала, их реализующего, в контексте сетевых угроз нарушения безопасности. Впервые в качестве организационно-правового обеспечения предложена дорожная карта реализации программы «Киберполигон» в различных аспектах проектной деятельности. Формализованное целеполагание проектных работ дает четкое практическое представление исследователю соответствия выявленных в аналогах противоречий, вытекающих из них задач и ожидаемых результатов их решения. В отличии от аналогов, пример обеспечения полигонных кибер-учений позволяет организовать моделирование эпидемических процессов в сетевых структурах с помощью различных программных инструментов, в том числе и для саморазмножающихся вирусов (модель «Бахчисарайский фонтан»).

Заключение

В заключении автор выражает надежду, что предложенное выше научно-методическом обеспечение будет полезно специалистам по защите информации в ходе эксплуатирования и развития атакуемых корпоративных сетей. Причем, стратегическим направлением его совершенствования представляется использование нейросетей как для выявления и классификации вторжений, так и для генерирования мер противодействия им на основе машинного обучения сети накопленным знаниям о мерах защиты корпоративных сетей. При этом необходим текущий риск-анализ ожидаемого ущерба от реализации выявленного сценария сетевой атаки.

Список литературы

1. Отчет о кибератаках на российские компании в 2022 году. URL: https://rt-solar.ru/analytics/reports/3332/ (дата обращения 12.09.2023).

2. Кибератаки на российские компании в I квартале 2023 года. URL: https://rt-

solar.ru/analytics/reports/3445/ (дата обращения 12.09.2023).

3. Ключевые уязвимости информационных систем российских компаний URL: https: //rt-solar.ru/analytics/reports/3386/ (дата обращения 12.09.2023).

4. Аграновский А. В. Основы технологии проектирования систем защиты информации в информационно-телекоммуникационных системах / А. В. Аграновский, В. И. Мамай, И. Г. Назаров и др. – Ростов-на-Дону: СКНЦ ВШ, 2016. – 258 с.

5. Бессонов А. Б. Организационно-правовое обеспечение информационной безопасности организации / А. Б. Бессонов // Научно-техническая информация. Серия 1: Организация и методика информационной работы. 2008. № 9. С. 16-28.

6. Бржезинская А. Д. Создание политики информационной безопасности и ее влияние на процесс управления безопасностью / А. Д. Бржезинская // Молодежный научный форум: Общественные и экономические науки. 2016. №11. С. 231–235.

7. Чернов А. Е. Основные требования и принципы, учитываемые при разработке и внедрении политики информационной безопасности / А. Е. Чернов // Вестник науки. 2023. Т. 2. № 6 (63).

8. Мельникова А. С. Главные особенности формирования политики информационной безопасности на предприятии / А.С. Мельникова // Вестник научных конференций. 2017. № 4-4(20). С. 86-87.

Московский государственный университет имени М.В. Ломоносова
Moscow State University named after M.V. Lomonosov

Поступила в редакцию 20.09.2023

Информация об авторе

Щербакова Дарья Владимировна – аспирант, Московский государственный университет имени М.В. Ломоносова, e-mail: alexanderostapenkoias@gmail.com

ORGANIZATIONAL AND LEGAL ASPECTS OF PROTECTION OF CORPORATE NETWORKS: SCIENTIFIC AND PRACTICAL REALITIES AND HORIZONS

D.V. Shcherbakova

The work discusses the protection of corporate networks. In this regard, the goal of this study was carried out with an emphasis on organizational and legal aspects. Methodological support for the fight against network invasions through the risk of the activities of corporate networks in terms of the formation of an adequate politician, regulations and instructions of protected organizations. Particular attention is paid to the formation of network counterintelligence, because all modern attacks are pre -prepared on the basis of data obtained during the implementation of network intelligence actions. In this regard, forms of appropriate regulation are proposed. The concept, functionality and architecture of the corporate training ground as a simulator of the organization's personnel during a network confrontation are considered.

Keywords: security, corporate network, security policy, security regulations, safety instructions, network counterintelligence, cyberpolygon.

Submitted 20.09.2023

Information about the author

Shcherbakova Daria V. – Graduate Student, Moscow State University named after M.V. Lomonosov, e-mail: alexanderostapenkoias@gmail.com