**DOI 10.36622/1682-7813.2024.27.2.004**
**УДК 004.056**

# ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ СЕТЕВОЙ КОНТРРАЗВЕДЫВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ КОРПОРАЦИИ (ЧАСТЬ I)

**Д.В. Щербакова, А.Ю. Пекло, А.С. Кривошеин, В.М. Питолин, О.Ю. Макаров, В.Н. Кострова**

Предлагается структура и содержание частной политики противодействия атакам типа «сетевая разведка». Выделены объекты защиты сетевой контрразведки. На основе анализа выделенных сочетаний вектора атаки и уязвимости сетевой разведки предложена обобщенная модель сетевого разведчика. Рассмотрены потенциальные меры противодействия выделенным сочетаниям сценарий-уязвимость. Представлены технологические компоненты, определяющиеся подсистемами защиты корпорации. Определены функции персонала корпорации по противодействию сетевой разведке. Предлагается система мер, обеспечивающая выполнение частной политики. Полученный документ может быть использован корпорацией для внутреннего организационно-правового обеспечения защиты от разведывательных действий со стороны злоумышленников.

Ключевые слова: частная политика, сетевая разведка, контрразведка, модель сетевого разведчика.

## Введение

Политика безопасности является одним из важнейших инструментов обеспечения информационной защиты корпорации на основе правил и рекомендаций противодействия кибератакам. Правильно разработанная и реализованная политика значительно уменьшает риски нарушения безопасности информации и помогает защитить корпорацию от негативных последствий [1].

Она включает множество частных политик, осуществляющих детализацию положений общей политики информационной безопасности применительно к основным объектам защиты [2].

В статье решается задача формирования частной политики информационной безопасности для защиты корпорации от атаки типа «сетевая разведка».

Для обеспечения информационной безопасности необходимо знать наиболее опасные объекты, векторы и уязвимости, используемые сетевой разведкой, и разработать для них частную политику [3].

Рассмотрим специфику формирования частной политики при защите корпорации от сетевой разведки.

## Объекты защиты и модель сетевого разведчика

Определим объекты доступа, подлежащие защите, для чего предлагается табл. 1.

Таблица 1

Объекты защиты

| Идентификатор объекта защиты | Объекты защиты |
|---|---|
| $O_1$ | Серверное оборудование |
| $O_2$ | Сетевое и телекоммуникационное оборудование |
| $O_3$ | Оборудование средств защиты информации |
| $O_4$ | TCP/UDP порты |
| $O_5$ | Сетевые службы |
| $O_6$ | Файлы журналов регистрации событий безопасности |
| $O_7$ | Конфигурационные файлы ПО и ОС |

На основе анализа выделенных сочетаний вектора атаки и уязвимости в табл. 2 предложена обобщенная модель нарушителя - сетевого разведчика. Данная модель относится к классу аналитических моделей и может использоваться в процессе формирования мер по противодействию сетевой разведке [4]. Модель нарушителя, также известная как профиль угрозы, является важной частью процесса анализа рисков нарушения ИБ. Эта модель описывает типы потенциальных злоумышленников, их цели, а также - мотивы, которыми они могут руководствоваться.

Таблица 2

Модель нарушителя при реализации сетевой разведки

| Идентификатор нарушителя | Тип нарушителя | Способ реализации | | Мотивация и цели нарушителя |
|---|---|---|---|---|
| | | Вектор атаки | Уязвимость | |
| $M_1$ | Провайдеры, поставщики оборудования | $VA_1$ | CWE-20 | Целью злоумышленника является получение списка IP-адресов и DNS имён, используемых в организации. Мотивацией преступника является использование одного и того же DNS имени для своего IP-адреса и для IP-адреса атакуемого устройства. Поскольку для обоих этих IP-адресов используется одно и тоже DNS имя, браузер помещает оба IP-адреса в одну и ту же зону безопасности и разрешает передачу информации между адресами |
| $M_2$ | Пользователи, авторизованные в системе | $VA_1$ | CWE-78 | Целью злоумышленника является получение нестандартного ответа от атакуемой системы с помощью реализации ICMP / IP по выявлению версии прошивки операционной системы или маршрутизатора на удаленном устройстве |
| $M_3$ | Администраторы безопасности | $VA_1$ | CWE-200 | Анализ процесса генерации уникального номера IP-пакета на удаленном хосте позволяет злоумышленнику определить операционную систему, используемую на хосте, с помощью проверки методом генерации идентификатора при отправке ответных пакетов |
| $M_4$ | Хакеры | $VA_1$ | CWE-287 | Злоумышленник посылает UDP-пакет с поддельным значением ID на закрытый порт целевой системы, чтобы получить сообщение об ошибке ICMP с отраженным значением ID. Таким образом, злоумышленник может определить характеристики операционной системы и использовать их в своих целях |

Продолжение табл.2

| Идентификатор нарушителя | Тип нарушителя | Способ реализации | | Мотивация и цели нарушителя |
|---|---|---|---|---|
| | | Вектор атаки | Уязвимость | |
| $M_5$ | Хакеры | $VA_2$ | CWE-20 | Для подготовки массированных атак на корпорацию необходимо осуществлять сбор информации о службах, компонентах, сервисах и приложениях атакуемой сети. При этом, главной целью злоумышленника является выявление уязвимых версий прошивок используемого сетевого оборудования. |
| $M_6$ | Пользователи систем и сетей | $VA_2$ | CWE-74 | Цель злоумышленник - найти уязвимость в утилите командной строки. Мотивом, в данном случае, является повышение привилегий до статуса «Администратора» |
| $M_7$ | Пользователи систем и сетей | $VA_2$ | CWE-200 | Для подключенных к сети устройств злоумышленник пытается использовать их уязвимости в контексте несанкционированного получения данных об элементах и ПО атакуемой сети. |
| $M_8$ | Хакеры | $VA_2$ | CWE-276 | Для правил фильтрации СЗИ злоумышленник будет пытаться использовать уязвимости для получения в удаленной атаке доступа к компонентам системы. |
| $M_9$ | Хакеры | $VA_2$ | CWE-862 | Целью является поиск уязвимостей в парольной защите устройств для сбора личной идентификационной информации |
| $M_{10}$ | Хакеры | $VA_3$ | CWE-20 | Сбор разведданных о жертве с помощью отправки синтаксически некорректных или нестандартных данных в попытке получить ответ, содержащий желаемые данные о сетевых службах |
| $M_{11}$ | Хакеры | $VA_3$ | CWE-78 | Цель злоумышленника с большой скорость отсканировать порты цели. Быстрое сканирование портов цели является серьезной угрозой для безопасности сетевых устройств, поскольку злоумышленник может проверять тысячи портов в секунду |

Продолжение табл.2

| Идентификатор нарушителя | Тип нарушителя | Способ реализации | | Мотивация и цели нарушителя |
|---|---|---|---|---|
| | | Вектор атаки | Уязвимость | |
| $M_{12}$ | Хакеры | $VA_3$ | CWE-200 | Злоумышленник применяет несколько способов для определения открытых портов на удаленном устройстве. Все службы и приложения, которые работают через протоколы TCP или UDP, будут иметь открытый порт, через который он сможет произвести обмен данными по сети |
| $M_{13}$ | Пользователи систем и сетей | $VA_3$ | CWE-862 | Цель злоумышленника - найти уязвимости в настройке контроля доступа в регистрах. Мотивом может служить использование неправильно настроенного контроля доступа в регистрах для чтения/ записи данных, которые не предназначены для получения или изменения пользователем. |
| $M_{14}$ | Пользователи систем и сетей | $\mathrm{VA}_4$ | CWE-20 | Объектами атаки выступают протоколы и синтаксис передачи данных для извлечения значимой информации. Мотивацией злоумышленника служит выявление функций и характеристик реализации протоколов связи |
| $M_{15}$ | Хакеры | $\mathrm{VA}_4$ | CWE-200 | Цель злоумышленника - инициировать установление потока данных или пассивно наблюдать за сообщениями, передаваемые по сети. Злоумышленник стремится установить поток данных или скрытно наблюдать за передачей сообщений в сети. Мотив заключается в получении конфиденциальной информации, необходимой для реализации последующих атак на жертву |

Окончание табл.2

| Идентификатор нарушителя | Тип нарушителя | Способ реализации | | Мотивация и цели нарушителя |
|---|---|---|---|---|
| | | Вектор атаки | Уязвимость | |
| $M_{16}$ | Хакеры | $VA_4$ | CWE-787 | Злоумышленник расшифровывает или декодирует информацию, содержащуюся в протоколах сетевого или прикладного уровня связи, которые используются для передачи данных между связанными узлами или системами в сети. Нарушитель не изменяет информацию в процессе передачи, так как его целью является получение разведывательных данных |

**Особенности обеспечения защиты**

В целях разработки частной политики, определяющей основные требования к системе защиты от сетевой разведки, рассмотрим потенциальные меры противодействия выделенным сочетаниям сценарий-уязвимость. Исходными данными для формирования перечня мер являются:

- выделенные объекты защиты (табл. 1);
- сформированная модель нарушителя, учитывающая наиболее опасные сочетания вектора сетевой разведки и уязвимости (табл. 2);
- рекомендации, предлагаемые нормативными документами ФСТЭК России;
- рекомендации с официально сайта CWE и CAPEC [5,6].

Технологические компоненты корпорации предусматривают подсистемы борьбы:

- со сканированием IP-адресов (далее – подсистема 1);
- с несанкционированным выявлением уязвимостей (далее – подсистема 2);
- с несанкционированным сканированием портов и сетевых служб (далее – подсистема 3);
- с прослушиванием сети (далее – подсистема 4).

Основные функции, реализуемые подсистемой 1:

- формирование списка IP-адресов, разрешенных для обмена сообщениями по протоколу ICMP;
- фильтрация ICMP-пакетов;
- блокировка сообщений ICMP, которые не требуются для нормального функционирования сети;
- всем устройствам корпорации должен быть присвоен уникальный DNS и IP-адрес.

Данные меры реализуются с помощью следующих средств защиты информации:

- межсетевых экранов (далее – МЭ);
- встроенных в ОС процедур фильтрации трафика.

Функции подсистемы 1 представлены на рис. 1.


Рис. 1. Функциональная схема подсистемы 1

Для своевременного обнаружения уязвимостей и проведения оценки состояния защищенности сети корпорации в ней разворачивается подсистема 2.

Подсистема 2 обеспечивает выявление уязвимостей в программно-аппаратной среде функционирования корпорации, опасные для реализации сетевой разведки. Выявление уязвимостей осуществляется путем сканирования адресного пространства сетевых узлов корпорации и используемых ими TCP/UDP портов, результаты которого сравниваются с сигнатурами известных уязвимостей [8].

Подсистема 2 обеспечивает функции по обнаружению несанкционированного сканирования уязвимостей в программно-аппаратной среде. Цель данной подсистемы предотвратить кибератаку, усложнив разведку злоумышленнику.

Данные меры, возможно реализовать с помощью следующих технических решений:

- ресурс, представляющий собой «приманку» для злоумышленника;
- сканер безопасности.

«Приманка» состоит из компьютера, операционной системы, приложений и данных, которые имитируют поведение системы и представляют ценность для потенциального злоумышленника, но на самом деле изолирована и контролируется при сборе информации.

«Приманки» могут быть использованы в исследовательских целях. Исследовательские «приманки» предназначены для проведения детального анализа хакерских атак и разработки средств для лучшей защиты от них. Исследовательские приманки обычно содержат данные с уникальными идентификаторами, которые помогают отслеживать украденные данные и выявлять связи между атаками и конкретными объектами.

«Приманки» не могут заменить другие механизмы безопасности, такие как брандмауэры, системы предотвращения вторжений, системы обнаружения вторжений, но они являются отличным дополнением к архитектуре безопасности. Это эффективный инструмент для сбора разведданных и выявления системных уязвимостей.

В свою очередь, сканер безопасности позволяет обнаруживать уязвимости независимо от программной и аппаратной платформы сканируемых сетевых узлов. Кроме этого, функционал сканера безопасности позволяет формировать не только отчет с указанием выявленных уязвимостей, но и ссылки на сайты с описанием обнаруженных уязвимостей.

Функции подсистемы 2 представлены на рис. 2.

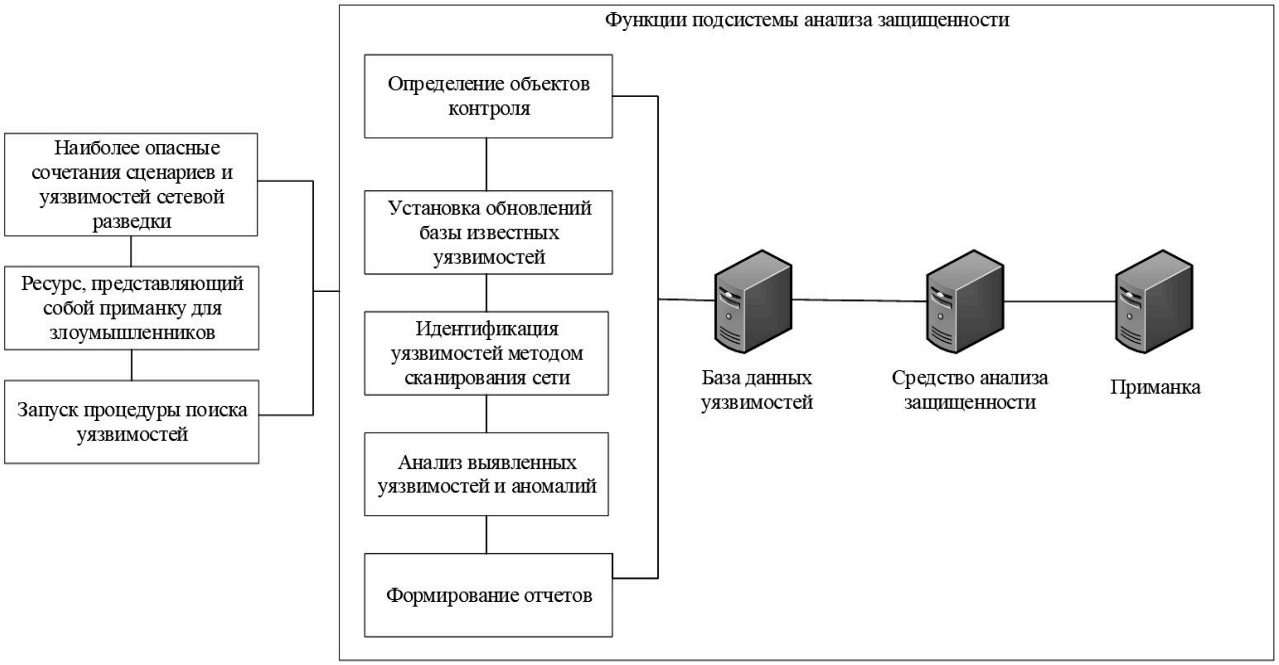


Рис. 2. Функциональная схема подсистемы 2

Подсистема 3 предназначена для защиты от угроз сетевой разведки, направленных на порты, сетевые службы, сервисы и основывается на системе управления доступом.

Основные функции, реализуемые подсистемой 3:

- контроль состояния портов устройств;
- предотвращение несанкционированного сканирования TCP/UDP портов;
- ограничение доступа к запущенным службам (только администратор должен иметь право запускать или останавливать службы);;
- контроль запуска сетевых служб и сервисов (должны быть запущенны только те службы, которые необходимы для работы используемого ПО на АРМ);
- анализ доступности в сети служб, версий ОС устройств и сервисов;
- управление доступом к сервисам и сетевым службам;
- блокирование несанкционированного доступа к сервисам и службам;
- для объектов доступа контроль их целостности;
- разграничение прав доступа удаленных пользователей для сетевых приложений, разграничение доступа;
- пресечение нарушений правил предоставления доступа;
- регистрация (логирование), обработка и хранение событий безопасности.

Функции подсистемы 3 представлены на рис. 3.


Рис. 3. Функциональная схема подсистемы 3

Подсистема 4 обеспечивает реализацию функций разграничения доступа к сетевым ресурсам корпорации, а также криптозащиту каналов связи, используемых для удаленного доступа к сетевому оборудованию организации.

Подсистема 4 обеспечивает: экранирование сети и криптозащиту её каналов.

Для защиты сетевых ресурсов применяются криптошлюзы, установленные на границе сетевого периметра серверной группы. В качестве дополнительных мер применяется сетевой коммутаторы с поддержкой технологии VLAN.

Таким образом, данная подсистема обеспечивает выполнение правил:

– по контролю доступа удаленных пользователей к ресурсам сетевых приложений;

– по снижению вероятности реализации актуальных угроз в процессах сетевого и межсетевого взаимодействия;

– по отслеживанию действий субъектов доступа на сетевом уровне;

– по обеспечению конфиденциальности и целостности информации, передаваемой по открытым каналам связи.

Функции подсистемы 4 представлены на рис. 4.

Перечисленные функции обеспечивают системный администратор и администратор безопасности. Распределение обязанностей сотрудников представлено в табл. 3.

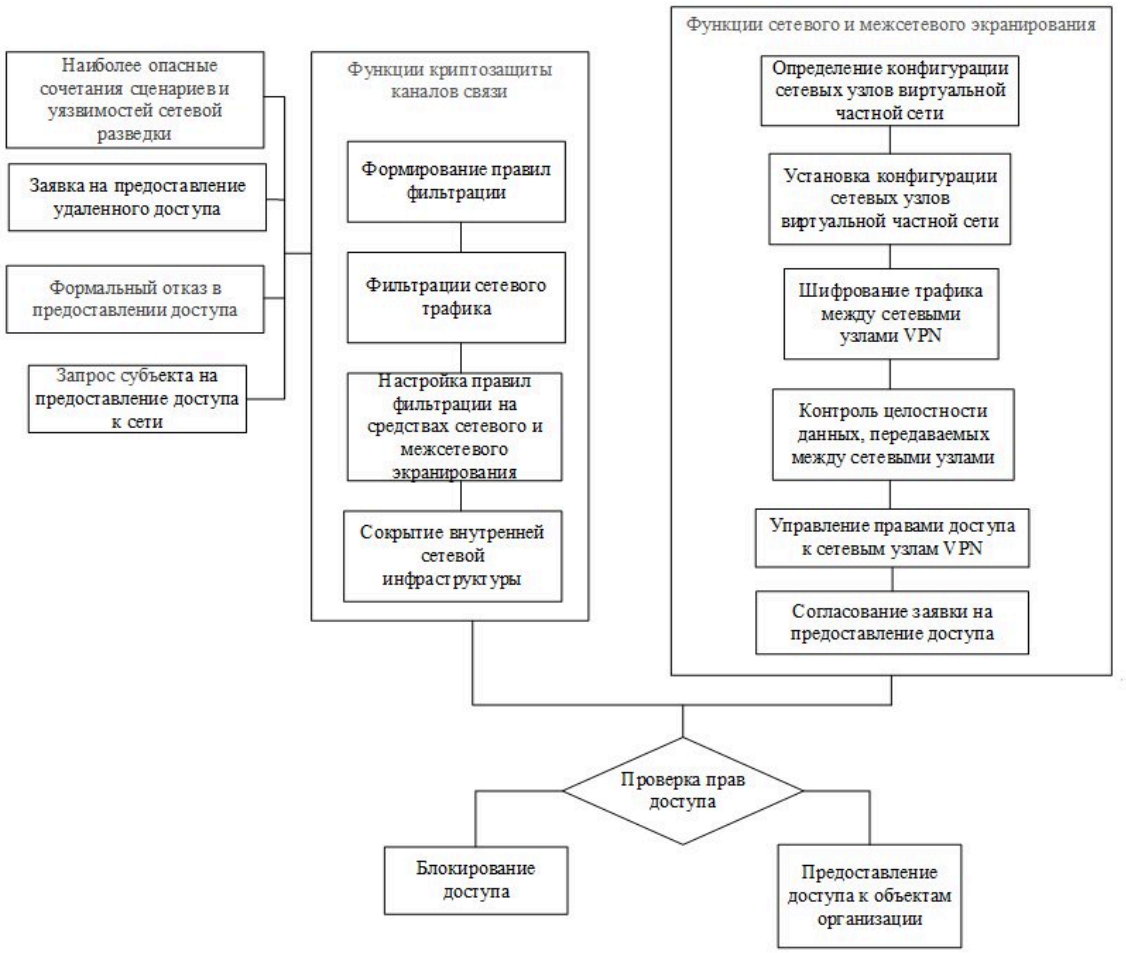


Рис. 4. Функциональная схема подсистемы 4

Таблица 3

Служебные обязанности лиц в подсистемах защиты

| Подсистема | Должность | |
|---|---|---|
| | Системный администратор | Администратор безопасности |
| Подсистема 1 | Формирование IP-адресов, по которым разрешен обмен сообщениями по протоколу ICMP | Создание правил фильтрации пакетов ICMP |
| Подсистема 2 | Создание для злоумышленников программной "приманки" | Контроль действий злоумышленника, "клюнувшего на приманку" |
| Подсистема 3 | Текущий анализ сетевых пакетов | Управление доступом к сервисам и сетевым службам |
| Подсистема 4 | Обеспечение экранирования и криптозащиты каналов связи | Разработка правил межсетевого экранирования |

Комплексная система мер и процедур состоит из действий, представленных в табл. 4, где указывается перечь мер и средств, необходимых для контроля выполнения требований, определенных Частной политикой для защиты от сетевой разведки.

Мероприятия по контролю выполнения мер, определенных в частной политике, а также проверка работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации должны проводиться на периодической основе и должны быть включены в ежегодный план мероприятий по защите информации. Причем сотрудники корпорации, назначенные ответственными за защиту информации, несут персональную ответственность за ненадлежащее исполнение или неисполнение положений настоящей политики.

Таблица 4

Меры противодействия и контроля в подсистемах защиты

| Подсистема | Меры противодействия | Меры контроля |
|---|---|---|
| Подсистема 1 | Фильтрование пакетов ICMP и блокировка сообщений ICMP, которые не требуются для нормального функционирования сети | Проверка IP-адресов и всех подключенных устройств в сервисе управления сетевым оборудованием |
| Подсистема 2 | Формирование множества ресурсов сети | Проведение регулярной проверки системы на соответствие заданным требованиям по безопасности, анализ уязвимостей и при необходимости исправление обнаруженных ошибок. |
| Подсистема 3 | Предотвращение несанкционированного сканирования TCP/UDP портов и ограничение доступа к запущенным службам | Мониторинг действий пользователей: контроль использования ресурсов и доступа к информации, фиксация несанкционированных действий. |
| Подсистема 4 | Разграничение доступа к сетевым ресурсам корпорации, а также криптозащита каналов связи, используемых для удаленного доступа к сетевому оборудованию организации. | Проверки работоспособности встроенных криптографических средств защиты информации и средств регистрации событий безопасности |

**Заключение**

Предложенное в настоящей работе формирование политики безопасности корпорации в следующих частях публикации будет детализировано до частных регламентов и инструкций. Таким образом будет реализовано трехступенчатое организационно-правовое обеспечение сетевой контрразведки корпорации. Подобное обеспечение может быть полезно для защиты корпораций различного профиля и масштаба, в контексте нарастающей опасности сетевой разведки, как известно, предваряющей многоплановые кибератаки. Всё это делает особенно актуальной регламентацию деятельности администраций корпоративных сетей по регистрации, реагированию и ликвидации последствий в отношении атак типа «сетевая разведка» (вторая часть настоящей работы), а также – подготовка инструктивных документов противодействия сетевой разведке (часть третья публикации). Совокупность подобных регламентирующих документов способна существенно укрепить информационную безопасность корпорации в условиях нарастающего противоборства, наблюдаемого ныне в глобальном и национальных кибернетических пространствах. Именно в такой парадигме приходится сегодня обсуждать, разрабатывать и реализовывать меры защиты корпоративных сетей, стремительно развивающихся и массированно атакуемых объектов цифровой инфраструктуры экономики.

**Список литературы**

1. Иерархическая структура документации по информационной безопасности. URL: https://safe-surf.ru/specialists/article/5244/626223/ (дата обращения: 12.01.24).

2. Сенцова А.Ю. Разработка частной политики информационной безопасности системы облачных вычислений / А.Ю. Сенцова, И.В. Машкина // Вестник Уфимского государственного авиационного технического университета. 2016. Т. 20. № 2(72). С. 134-142.

3. Кузьменко, И. Я. Инструкция по обеспечению информационной безопасности в организациях / И. Я. Кузьменко, А. С. Власюк // Инновации. Наука. Образование. 2021. № 35. С. 99-104.

4. Методический документ ФСТЭК России «Методика оценки угроз безопасности информации» [Электронный ресурс] URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021 (дата обращения: 12.01.24).

5. Список CWE версии 4.10 URL: https://cwe.mitre.org/data/index.html (дата обращения: 12.01.24).

6. Common Attack Pattern Enumeration and Classification URL: https://capec.mitre.org/index.html (дата обращения: 12.01.24).

7. Сканирование сетей URL: https://compress.ru/article.aspx?id=16249 (дата обращения: 12.01.24).

8. Выявление сетевых уязвимостей сканированием портов ПК URL: https://studopedia.ru/29_57943_viyavlenie-setevih-uyazvimostey-skanirovaniem-portov-pk.html (дата обращения: 12.01.24).

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

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 07.02.2024

**Информация об авторах**

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

**Пекло Арина Юрьевна** – студентка, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

**Кривошеин Александр Сергеевич** – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

**Питолин Владимир Михайлович** – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

**Макаров Олег Юрьевич** – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

**Кострова Вера Николаевна** – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

# ORGANIZATIONAL AND LEGAL SUPPORT OF NETWORK COUNTERINTELLIGENCE ACTIVITIES OF THE CORPORATION (PART I)

**D.V. Shcherbakova, A.Yu. Peklo, A.S. Krivoshein, V.M. Pitolin, O.Yu. Makarov, V.N. Kostrova**

The structure and content of a private policy of counteracting attacks of the type “network intelligence” is proposed. The regulatory framework and objects of protection of network counterintelligence has been allocated. Based on the analysis of the selected combinations of the attack vector and vulnerability of network intelligence, a generalized model of a network intelligence officer was proposed. Potential measures to counteract the selected combinations scenario-vulnerability are considered. The technological components are represented that are determined by the corporation protection subsystems from network intelligence. The functions of the roles of the technical personnel of the organization to ensure protection against network intelligence were highlighted. A comprehensive system of measures and procedures is proposed that is responsible for monitoring the implementation of requirements determined by private policy. The resulting document can be used to develop internal documents of the corporation, which contain detailed clarification of the provisions to protect the network from reconnaissance actions by the attacker.

Keywords: private policy, network intelligence, counterintelligence, model of a network intelligence officer.

Submitted 07.02.2024

**Information about the authors**

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

**Arina Yu. Peklo** –student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

**Alexander S. Krivoshein** – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

**Vladimir M. Pitolin** – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

**Oleg Yu. Makarov** – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

**Vera N. Kostrova** – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com