DOI 10.36622/VSTU.2023.26.2.008
УДК 004.056.57

АТАКИ ТИПА «СЕТЕВАЯ РАЗВЕДКА»: РИСК-ЛАНДШАФТ И ЧАСТНАЯ ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

А.Ю. Пекло, Г.А. Остапенко, Д.В. Щербакова, А.А. Остапенко

В работе рассматривается специфика построения частной политики в части защиты сети предприятия от сетевой разведки в соответствии с риск-ландшафтом. Сформировано полное множество сценариев и уязвимостей сетевой разведки. На основании статистики, частоты и ущербности атак выявлены наиболее опасные сочетания сценариев и уязвимостей заданного типа атаки. Построен риск-ландшафт реализации сетевой разведки. В результате предлагается специфика частной политики защиты сети организации от сетевой разведки, учитывающая наиболее опасные сочетания векторов и уязвимостей заданного типа атаки. Предложенная специфика может быть использована для разработки внутренних документов организации, в которых содержатся детальные разъяснения положений по защите сети от разведывательных действий со стороны киберзлоумышленника.

Ключевые слова: сетевая разведка, уязвимость, сценарий атаки, риск-ландшафт, частная политика.

Введение

Сетевая разведка является неотъемлемой частью практически всякой кибератаки, и даже при использовании наилучших мер защиты безопасности всегда есть вероятность несанкционированного проникновения в корпоративную сеть.

Рассматриваемый тип атаки позволяет получить информацию о топологии сети, технических характеристиках серверов, автоматизированных рабочих мест, сетевого оборудования, а также об их уязвимостях и способах защиты атакуемой сети.

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

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

По-прежнему актуальна проблема пренебрежения качеством организационно-правого обеспечения в отечественных организаций. 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 риски, вводя сотрудников в заблуждение [1].

В целях устранения этих рисков для организации предлагается модернизировать подход к составлению её частной политики информационной безопасности для защиты от сетевой атаки типа сетевая разведка (Политика).

В соответствии с поставленной для достижения цели задачей, необходимо:

на основании статистики частоты и ущербности атак сетевой разведки выявить наиболее опасные сочетания сценариев и уязвимостей, с которыми может столкнуться компания при обеспечении информационной безопасности,

для выявленных наиболее опасных сочетаний сценариев и уязвимостей разработать Политику и, в соответствии с ней, внести необходимые корректировки в

регламенты и инструкции по защите корпоративной сети.

Формирование и описание полного множества сценариев сетевой разведки

Зачастую перед атакой проводится сетевая разведка, в ходе которой злоумышленник пытается собрать необходимые для атаки сведения. В зависимости от сценария атаки набор сведений может меняться.

В целях формирования полного множества сценариев атаки применяются несколько руководящих документов, последний из которых принят в 2021 году – «Методика оценки угроз безопасности информации» (Методика). Приведенная в нём методика предлагает использовать (при определении тактики злоумышленника) массивы данных о признаках угроз, а затем, ориентируясь на экспертное мнение, формировать векторы атак с возможностью заимствования различных, в том числе, зарубежных способов описания сценариев реализации атаки [2]. В этой связи осуществляется сбор информации о существующих уязвимостях и возможных сценариях атаки, которые могут использоваться для разработки мер по противодействию.

В интересах формирования вектора сетевой разведки проведем анализ классификационных схем сетевых атак: Mitre Att&ck, CAPEC, NIST 800-115 [3-5].

Для формирования полного множества сценариев сетевой разведки следует проанализировать выделенные методологии с целью выделения конкретных сценариев атаки.

Согласно [3-5] цели сетевой разведки могут быть различными, но обычно они связаны с определением архитектуры и характеристик сети, а также выявлением ее уязвимостей и возможных угроз. Основные цели сетевой разведки могут включать в себя следующие моменты:

определение размера и топологии сети,

выявление слабых мест и уязвимостей, таких как устаревшие программы и открытые порты,

оценка уровня безопасности сети,

анализ доступных сервисов и приложений,

сбор информации о производительности сети и ее загрузке,

выявление возможных угроз для безопасности сети,

проверка соответствия политике безопасности,

оценка готовности сети к атакам и разработка планов мероприятий по укреплению защиты,

подбор кандидатов для атаки на сеть,

определение маршрутов и устройств, включенных в сеть.

Исходя из целей и тактик сетевой разведки, можно выделить следующие сценарии атаки типа сетевая разведка [6].

Сканирование диапазона IP-адресов

Злоумышленник определяет диапазон IP-адресов, который используется в корпоративной сети с помощью запросов доменных сетевых имён. При помощи утилиты ping (или аналогичных программ) хосту назначения посылается команда ECHO_REQUEST протокола ICMP. Ответное сообщение ECHO_REPLY говорит о том, что узел доступен. Это самый простой и часто используемый метод идентификации узлов.

Получив полный список активных IP-адресов, злоумышленник сможет подключиться к устройству напрямую. Кроме того, узнав внешний IP-адрес, злоумышленник может изменить настройки доступа в Интернет, например, настроить маршрутизатор так, что вместо оригинала сайта будут открываться его копия.

Обнаружение уязвимостей

Уязвимости представляют наибольшую ценность для злоумышленников. В 2022 году установлен отрицательный рекорд: по данным NIST, было верифицировано более 25 тысяч новых уязвимостей. Рост числа уязвимостей связан с несоблюдением принципов безопасной разработки нового программного обеспечения (ПО).

На первом этапе злоумышленник исследует уязвимости операционной системы (ОС).

На следующем этапе производится сканирование установленного ПО. Для каждого ПО определяется, является ли оно

уязвимым. Выявление уязвимостей производится на основании сравнения состояния системных параметров сканируемого программного обеспечения (или его компонентов) с базой уязвимостей, используемой сканером.

Помимо уязвимостей ОС и ПО злоумышленник рассматривает возможности использования недостатков сетевого оборудования. Специалисты редко проверяют настройки маршрутизатора, так как проверка сетевой безопасности в организации, зачастую, направлена на компьютеры сотрудников, поэтому факт несанкционированного доступа к сетевому оборудованию долго остается незамеченным.

На заключительном этапе производится тестирование способов эксплуатации найденных уязвимостей – тестирование на проникновение. Злоумышленник выделяет уязвимости, использование которых принесет наибольший ущерб атакуемой организации.

Сканирование портов и определение сетевых служб

Согласно статистике компании, «Лаборатория Касперского», сканирование портов занимает 2 место среди нарушений сетевой безопасности.

Цель данного подхода – выявить открытые TCP/UDP порты, обнаружить сервисы, ответственные за открытое состояние порта, и собрать всю доступную информацию о хосте.

При таком сценарии злоумышленник получает информацию о системе защиты корпоративной сети: используются ли межсетевые экраны, прописаны ли правила фильтрации трафика, установлены ли средства защиты информации. Воздействие на выявленные сетевые службы способно обеспечить считывание информации, блокирование устройства или полный над ним контроль.

Прослушивание сети

Это акт перехвата и мониторинга трафика в сети с помощью программного обеспечения, которое фиксирует все пакеты данных, проходящие через данный сетевой интерфейс, или с помощью аппаратных устройств, специально предназначенных для этой цели. Цель состоит в том, чтобы украсть информацию, как правило, идентификаторы пользователей, пароли, детали о сети.

Сформированное множество сценариев содержит выделенные, в соответствие с рассмотренными методологиями, сценарии атаки. При этом, целесообразно было включить в перечень общие для каждой классификации тактики, исключить маловероятные сценарии и дополнить его уникальными для каждой классификации способами реализации атаки. Таким образом, вектор сетевой разведки можно представить в виде множества:

$$A = \{VA_1, VA_2, VA_3, VA_4\}, \qquad (1)$$

где VA_1 – сканирование диапазона IP-адресов,

VA_2 – обнаружение уязвимостей,

VA_3 – сканирование портов и определение сетевых служб,

VA_4 – прослушивание сети.

Формирование и описание полного множества уязвимостей, используемых для реализации сетевой разведки

Действующими нормативными и методическими документами в области защиты информации установлено, что каждая угроза безопасности информации в общем виде описывается через возможности нарушителя и используемые нарушителем уязвимости. Эксплуатируя уязвимость, атакующий получает возможность реализовать атаку.

На сегодняшний день официально признанные реестры уязвимостей: отечественный ресурс – банк данных угроз безопасности информации (БДУ) ФСТЭК России и национальная база данных США NVD.

Появление отдельных баз данных и реестров уязвимостей, которые не взаимодействуют между собой, привело к проблеме несогласованности информации, включая неоднозначную идентификацию уязвимостей, а также различия в классификации и оценке уязвимостей. Так, согласно принятой форме описания уязвимости в БДУ ФСТЭК России, каждую

уязвимость можно отнести к одному из способов эксплуатации, взятых из международного стандарта CAPEC. Сведения об уязвимостях, содержащиеся в базе данных NVD и в стандарте CAPEC, не имеют прямой связи. Однако определить такую связь возможно через типы ошибок CWE, которые связывают упомянутые реестры уязвимостей. Таким образом, для формирования и описание полного множества уязвимостей, используемых для реализации сетевой разведки, целесообразнее рассмотреть стандарты CAPEC и CWE [7,8].

Многие шаблоны атак основываются на представлении CWE, так как этот перечень наиболее структурированный и полный. Шаблон атаки в CAPEC включает описание способов использования уязвимостей, возможных негативных последствий и методов противодействия. Кроме того, в описании указываются соответствующие уязвимости из CVE и приводящие к ним недостатки из CWE.

По целям сетевой разведки, из классификации CAPEC можно выделить категорию, которая относится к виду атаки «Сбор и анализ информации», содержащая шаблоны, которым присвоен идентификатор. Для формирования множества уязвимостей сетевой разведки следует рассмотреть шаблоны атак из выбранной категории CAPEC и найти связь с представлением уязвимостей согласно стандарту CWE. Множество уязвимостей, представленное в табл. 1, определяет направление атаки, которое может использоваться злоумышленником для реализации сетевой разведки. Он определяется набором уязвимостей в системе, которые могут быть использованы для доступа к конкретным ресурсам или для выполнения определенных действий. Составленное множество уязвимостей является фундаментом при составлении политик информационной безопасности, так как на основании его анализа специалисты по защите информации могут оценить потенциальные угрозы и разработать соответствующие регламенты и инструкции по защите сети организации от сетевой разведки [4,6].

Таблица 1

Множество уязвимостей, используемых для реализации сетевой разведки

Идентификатор уязвимости	Наименование уязвимости
CWE-20	Недостаточная проверка вводимых данных
CWE-74	Неверная нейтрализация вредоносных элементов в входных данных
CWE-78	Внедрение команды ОС
CWE- 200	Раскрытие информации
CWE-209	Утечка информации в сообщениях об ошибках
CWE-276	Неправильные разрешения по умолчанию
CWE-287	Неправильная аутентификация
CWE-302	Обход аутентификации посредством неизменяемых данных
CWE-311	Непринятие мер по шифрованию секретных данных
CWE-319	Передача секретной информации в виде открытого текста
CWE-345	Недостаточная проверка подлинности данных
CWE-346	Ошибка подтверждения источника данных
CWE-352	Межсайтовая фальсификация запросов
CWE-384	Фиксация сеанса
CWE-522	Недостаточно защищенные учетные данные
CWE-693	Нарушение механизма защиты данных
CWE-787	Запись за пределы допустимого диапазона
CWE-862	Отсутствует авторизация

Риск-ландшафт реализации сетевой разведки

Для риск-анализа сетевой разведки прежде всего, необходимо установить соответствие между векторами сетевой разведки (1) и множеством уязвимостей (табл. 1). Это представляется возможным сделать с помощью матрицы смежности (рис. 1).

	VA_1	VA_2	VA_3	VA_4
CWE-20	1	1	1	1
CWE-74	0	1	0	0
CWE-78	1	0	1	0
CWE-200	1	1	1	1
CWE-209	0	0	0	1
CWE-276	1	1	0	0
CWE-287	1	0	0	1
CWE-302	1	0	1	1
CWE-311	0	1	0	0
CWE-319	0	1	0	1
CWE-345	0	0	0	1
CWE-346	1	1	0	0
CWE-352	1	0	1	1
CWE-384	1	0	0	1
CWE-522	0	1	0	0
CWE-693	1	0	1	1
CWE-787	0	0	0	1
CWE-862	1	1	0	0

Рис. 1. Матрица смежности сценариев атак и уязвимостей

В методическом плане риск-оценка сетевой разведки может быть осуществлен на основе следующих обозначений:

VA_{si} – i-ый вектор сетевой разведки,

VB_{sj} – j-ыя уязвимость, используема для реализации сетевой разведки,

$Risk_{sij}$ – риск реализации сетевой разведки посредством i-го вектора на j-ую уязвимость,

F_{sij} – частота успешного использования j-ой уязвимости при реализации сетевой разведки посредством i-го вектора,

K_{sij} – уровень критичности уязвимости,

Δt_{si} – среднестатистическое значение простоя атакуемой сети в результате успеха сетевой разведки посредством i-го вектора.

С учетом введенных обозначений вероятность реализации атаки типа сетевая разведка посредством i-го вектора на j-ую уязвимость может быть оценена выражением:

$$P_{sij} = \frac{F_{sij}}{\sum_j F_{sij}}. \quad (2)$$

В свою очередь, ущерб может быть оценен следующим образом:

$$U_{sij} = \frac{K_{sij}}{\sum_j K_{sij}} \times \Delta t_{si}. \quad (3)$$

Тогда риск будет равен:

$$Risk_{sij} = P_{sij} \times U_{sij}. \quad (4)$$

Данные по частоте F_{sij} представляют собой анализ списка уязвимостей из БДУ ФСТЭК [9].

Относительно ущерба можно заметить следующее. Обнаружение сетевых вторжений и классификация атак — это область активных исследований, но основной проблемой для исследователя является недоступность наборов данных, которые имитируют сетевой трафик, на основании которого можно оценить ущерб. Набор данных UNSW-NB15 был создан с целью устранения этого пробела. Среднестатистические значения простоя Δt_{si}, может быть представлены выборкой по выделенным векторам сетевой разведки в соответствии с их классификацией в UNSW-NB15 [10].

При этом, уровень критичности уязвимости K_{sij} рассчитать достаточно затруднительно, так как основополагающими данными для его расчета являются сведения о составе и архитектуре информационных ресурсов организации, полученные по результатам их инвентаризации [11]. Поэтому подход (2) – (4) уместно несколько трансформировать. Здесь можно учесть тот факт, что успехи атак через различные уязвимости обычно являются вероятностно несовместимыми событиями. Если принять подобное предположение за основу, то искомая вероятность будет равна:

$$P_{sij} = \sum_j F_{sij}, \quad (5)$$

т. е. сумме всех частот использования уязвимостей, соответствующих заданному типу атак и рассматриваемому i-му вектору.

В свою очередь, коэффициент, учитывающий долю j-й уязвимости, можно также трансформировать:

$$U_{sij} = \frac{F_{sij}}{\sum_j F_{sij}} \times \Delta t_{si}. \quad (6)$$

Заменим K_{sij} на F_{sij}. Тогда из (5) и (6) выражение риска примет следующий вид:

$$Risk_{sij} = \sum_j F_{sij} \times \frac{F_{sij}}{\sum_j F_{sij}} \times \Delta t_{si} = \\ = F_{sij} \times \Delta t_{si}\,. \quad (7)$$

Разделив выражение (7) на максимальное значение Δt_{si}, можно получить нормированный риск:

$$\overline{Risk_{sij}} = F_{sij} \times \frac{\Delta t_{si}}{\max[\Delta t]} = \\ = F_{sij} \times \overline{U_{sij}}. \quad (8)$$

Отсюда рассчитаем значения F_{sij} и $\overline{U_{sij}}$ для сетевой разведки (табл. 2 и 3).

Таблица 2

Частота успешного использования j-ой уязвимости при реализации сетевой разведки

Идентификатор уязвимости	F_{sij}
CWE-20	0,1177
CWE-74	0,0069
CWE-78	0,0206
CWE- 200	0,0456
CWE-209	0,0081
CWE-276	0,0042
CWE-287	0,0209
CWE-302	0,0003
CWE-311	0,0006
CWE-319	0,0048
CWE-345	0,0080
CWE-346	0,0003
CWE-352	0,0072
CWE-384	0,0003
CWE-522	0,0042
CWE-693	0,0012
CWE-787	0,0560
CWE-862	0,0098

Таблица 3

Ущерб от реализации сетевой разведки

Идентификатор сценария атаки	$\overline{U_{sij}}$
VA_1	0,3679
VA_2	0,8105
VA_3	0,4065
VA_4	0,7254

На основе полученных данных по частоте и ущербности сетевой разведки преобразуем матрицу смежности в матрицу рисков (рис. 2).

	VA_1	VA_2	VA_3	VA_4
CWE-20	0,0433	0,0954	0,0478	0,0854
CWE-74	-	0,0056	-	-
CWE-78	0,0076	-	0,0084	-
CWE-200	0,0168	0,0370	0,0185	0,0331
CWE-209	-	-	-	0,0059
CWE-276	0,0015	0,0034	-	-
CWE-287	0,0077	-	-	0,0152
CWE-302	0,0001	-	0,0001	0,0002
CWE-311	-	0,0005	-	-
CWE-319	-	0,0039	-	0,0035
CWE-345	-	-	-	0,0058
CWE-346	0,0001	0,0002	-	-
CWE-352	0,0026	-	0,0029	0,0052
CWE-384	0,0001	-	-	0,0002
CWE-522	-	0,0034	-	-
CWE-693	0,0004	-	0,0005	0,0009
CWE-787	-	-	-	0,0406
CWE-862	0,0036	0,0079	-	-

Рис. 2. Матрица рисков реализации атак через уязвимости

С помощью рис. 2 построим риск-ландшафт реализации сетевой разведки (рис. 3). Он представляет собой графическое отображение рисков всех комбинаций сценариев и уязвимостей сетевой разведки. Этот инструмент визуально показывает все возможные риски от реализации заданного типа атаки.

Риск-ландшафт поможет персоналу организации понять, с какими рисками он может столкнуться при сетевой разведке. Рис. 3 демонстрирует, какие риски являются наиболее критичными и требуют более тщательного мониторинга и управления.

В целом, риск-ландшафт является важным инструментом при формировании

Политики, так как он позволяет организации заранее определить потенциальные проблемы и разработать меры по их разрешению.

Согласно рис. 3 можно выделить 16 наиболее опасных сочетаний сценариев и уязвимостей, представленных в табл. 4.

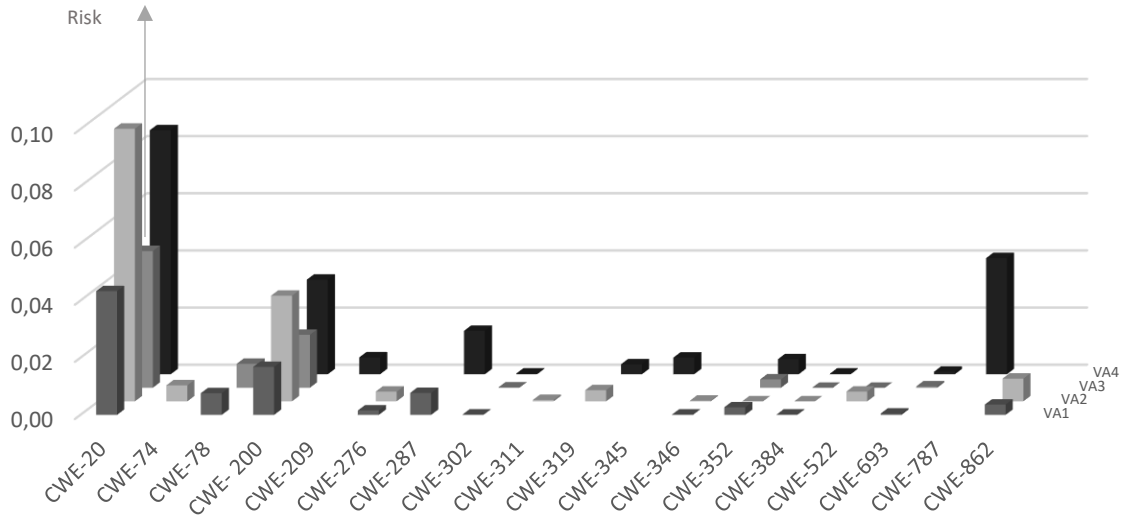

Рис. 3. Риск-ландшафт реализации сетевой разведки

Таблица 4

Наиболее опасные сочетания сценариев и уязвимостей сетевой разведки

Идентификатор вектора атаки	Наименование вектора атаки	Идентификатор уязвимости	Наименование вектора уязвимости
VA_1	Сканирование диапазона IP-адресов	CWE-20	Недостаточная защита данных
		CWE-78	Внедрение команды ОС
		CWE-200	Раскрытие информации
		CWE-287	Неправильная аутентификация
VA_2	Обнаружение уязвимостей	CWE-20	Недостаточная проверка вводимых данных
		CWE-74	Неверная нейтрализация вредоносных элементов в выходных данных
		CWE-200	Раскрытие информации
		CWE-276	Неправильные разрешения по умолчанию
		CWE-862	Отсутствует авторизация
VA_3	Сканирование портов и определение сетевых служб	CWE-20	Недостаточная проверка вводимых данных
		CWE-78	Внедрение команды ОС
		CWE-200	Раскрытие информации
		CWE-862	Отсутствует авторизация
VA_4	Прослушивание сети	CWE-20	Недостаточная защита данных
		CWE-200	Раскрытие информации
		CWE-787	Запись за пределы допустимого диапазона

Специфика частной политики при защите предприятия от сетевой разведки

Политика определяет стратегию и тактику построения системы защиты организации от сетевой разведки. Стратегический компонент связан с выбором информационных технологий и ПО для достижения определенных бизнес-целей. Тактическая часть, в свою очередь, подробно описывает правила обеспечения безопасности, в соответствии с сформированным риск-ландшафтом.

Выбор нормативной базы, на которой строится разработка Политики, зададут правильный вектор на создание системы защиты от сетевой разведки. Серия стандартов ГОСТ Р ИСО/МЭК 27ххх содержит перечень документов по различным направлениям системы менеджмента информационной безопасности: техническое, стратегическое, организационное. Эти стандарты определяют основные требования, принципы и практики для управления рисками, связанными с защитой конфиденциальности, целостности и доступности информации в организации. Кроме того, они определяют методы и процедуры для оценки, управления и непрерывного улучшения системы управления ИБ. Таким образом, предлагаемая нормативная база для составления Политики позволяет применять стандарт для нейтрализации угроз сетевой разведки в организациях любого масштаба и уровня нормативного регулирования [12].

Требования к технологическому и организационному обеспечению защиты организации от сетевой разведки

Технологические и организационные компоненты определяются составом следующих подсистем защиты организации на основании выделенных сочетаний сценариев и уязвимостей сетевой разведки:

подсистема защиты от сканирования диапазона IP-адресов (подсистема 1);

подсистема защиты от несанкционированного обнаружение уязвимостей (подсистема 2);

подсистема защиты от несанкционированного сканирование портов и определение сетевых служб (подсистема 3);

подсистема защиты от прослушивания сети (подсистема 4) [13].

Требования к функционалу Подсистем представлены на рис. 4-7.

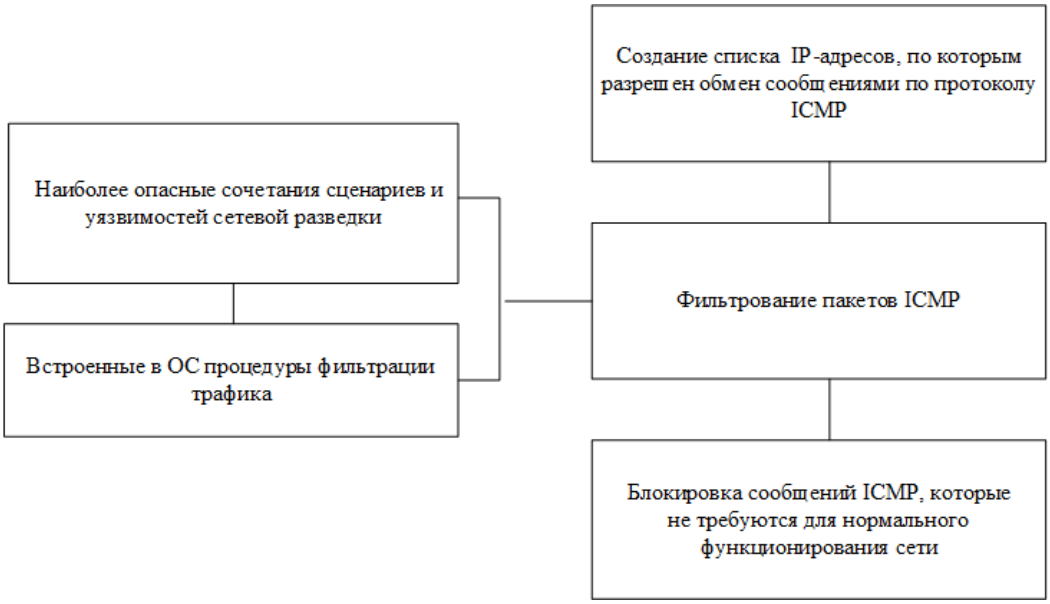

Рис. 4. Функциональная схема Подсистемы 1

Рис. 5. Функциональная схема Подсистемы 2

Рис. 6. Функциональная схема Подсистемы 3

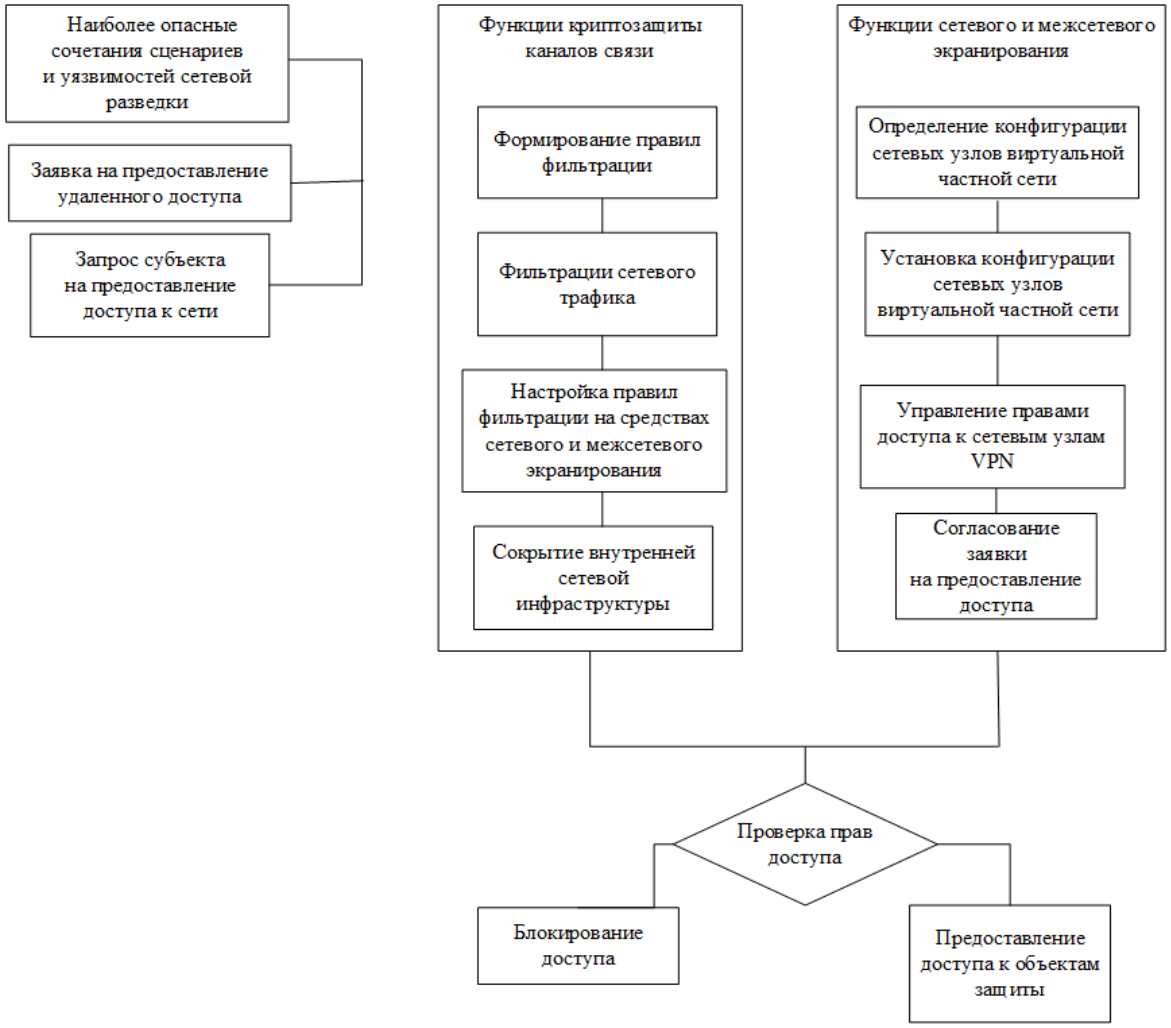

Рис. 7. Функциональная схема Подсистемы 4

Роли и обязанности, связанные с обеспечением информационной безопасности организации в части защиты от сетевой разведки

На основании выделенных подсистем защиты от сетевой разведки в составе персонала требуется выделение следующих лиц, обеспечивающих защиту от сетевой разведки (табл. 5).

Определение документов, содержащих требования к процедурам обеспечения ИБ, выполняемым работниками в рамках технологических процессов, реализующих технологии, требования ИБ, к которым определены частной политикой

В рамках реализации положений, развития и детализации Политики должны быть разработаны следующие документы третьего уровня:

– регламент определяет порядок регистрации и подтверждения возникновения инцидентов безопасности, произошедших в организации в ходе реализации сетевой разведки,

– регламент определяет порядок реагирования на инциденты безопасности, произошедших в организации в ходе реализации сетевой разведки,

– регламент определяет порядок ликвидации последствий инцидентов безопасности, произошедших в Организации в ходе реализации сетевой разведки,

– должностные инструкции по защите информации в организации в рамках противодействия сетевой разведки.

Таблица 5

Функции ролей технического персонала организации для обеспечения защиты от сетевой разведки

Подсистема	**Должность**	
	Системный администратор	Администратор безопасности
Подсистема 1	Создание списка IP-адресов, по которым разрешен обмен сообщениями по протоколу ICMP	Создание правил фильтрации пакетов ICMP
Подсистема 2	Разработка и поддержание работоспособности ресурса, представляющего собой «приманку» для злоумышленников	Исследования поведения злоумышленника после его проникновения внутрь корпоративной сети с помощью «приманки»
Подсистема 3	Анализ объема и содержания данных сетевых пакетов	Управление доступом к сервисам и сетевым службам
Подсистема 4	Установка и настройка ПО межсетевого экранирования и криптозащиты каналов связи	Разработка правил межсетевого экранирования

Заключение

Основными полученными результатами являются:

– сформирован риск-ландшафта для наиболее опасных сочетаний сценариев и уязвимостей сетевой разведки,

– разработана специфика частной политики в части защиты сети предприятия от сетевой разведки.

При этом новизна работы заключается в использовании риск-ландшафта для формирования частной политики информационной безопасности. Приведенная специфика частной политики, в части защиты сети предприятия от сетевой разведки, относится к методам нападения путем реализации механизмов, направленных на прямое получение данных о сетевых объектах. Разработанная Политика может быть использована для анализа опасности указанных механизмов для конкретных корпоративных сетей.

Перспективным направлением настоящего исследования является использование приведенной специфики организацией для разработки внутренних документов, в которых содержатся детальные разъяснения положений по защите сети от сетевой разведки.

Соблюдение требований предложенной частной политики безопасности позволит существенно снизить риски разведывательных действий со стороны злоумышленника.

Список литературы

1. Остапенко А.Г. Направление совершенствования нормативно-правового обеспечения объектов информатизации на основе риск-анализа их кибербезопасности / А.Г. Остапенко, Д.В. Щербакова, Д.А. Нархов, Ю.В. Макаров, А.С. Кривошеин // Информация и безопасность. 2022. Т. 25, № 4. С. 539-598.

2. Методика оценки угроз безопасности ФСТЭК России. URL: https://fstec.ru/ (дата обращения 10.06.2023).

3. ATT&CK Matrix for Enterprise URL: https://attack.mitre.org/ (дата обращения 23.04.2023).

4. Common Attack Pattern Enumeration and Classification URL: https://capec.mitre.org/index.html (дата обращения 23.04.2023).

5. SP 800-115. Technical Guide to Information Security Testing and Assessment URL: https://csrc.nist.gov/publications/detail/sp/800-115/final (дата обращения 23.04.2023).

6. Пахомова А.С. Об использовании классификации известных компьютерных атак в интересах разработки структурной модели компьютерной разведки / А.С. Пахомова, А.П. Пахомов, В.Г. Юрасов // Информация и безопасность. 2013. Т. 16, № 1. С. 81-86.

7. Список CWE версии 4.10 URL: https://cwe.mitre.org/data/index.html (дата обращения 23.04.2023).

8. Common Attack Pattern Enumeration and Classification URL:

https://capec.mitre.org/index.html (дата обращения 23.04.2023).

9. Банк данных угроз безопасности информации URL: https://bdu.fstec.ru/threat (дата обращения 23.04.2023).

10. UNSW_NB15 URL: https://www.kaggle.com/datasets/ (дата обращения 10.06.2023).

11. Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств (утв. Федеральной службой по техническому и экспортному контролю 28 октября 2022 г.).

12. Иерархическая структура документации по информационной безопасности URL: https://safe-surf.ru/specialists/article/5244/626223/ (дата обращения 23.04.2023).

13. Оюн Ч.О. Основные подходы к формированию политики безопасности / Ч.О. Оюн, Е.В. Попантонопуло, И.Н. Карманов // Интерэкспо Гео-Сибирь. 2019. Т. 6, № 2. С. 3-7

Воронежский государственный технический университет
Voronezh State Technical University

Финансовый университет при Правительстве Российской Федерации
Financial University under the Government of the Russian Federation

Поступила в редакцию 03.05.2023

Информация об авторах

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

Остапенко Григорий Александрович – д-р техн. наук, проректор Финансового университета при Правительстве Российской Федерации, e-mail: alexanderostapenkoias@gmail.com

Щербакова Дарья Владимировна – соискатель, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Остапенко Александр Алексеевич – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

ATTACKS SUCH AS «NETWORK RECONNAISSANCE»: RISK LANDSCAPE AND PRIVATE INFORMATION SECURITY POLICY

A.Yu. Peklo, G.A. Ostapenko, D.V. Shcherbakova, A.A. Ostapenko

The article considers the specifics of building a private policy in terms of protecting the enterprise network from network exploration in accordance with the risk landscape. A complete set of network intelligence scenarios and vulnerabilities has been formed. Based on statistics, frequency and flaw, the most dangerous combinations of scenarios and vulnerabilities of a given type of attack were identified. A risk landscape for the implementation of network intelligence has been built. As a result, the specifics of private policy are proposed in terms of protecting an enterprise's network from network intelligence, taking into account the most dangerous combinations of vectors and vulnerabilities of a given type of attack. The proposed specifics can be used to develop internal documents of the organization, which contain detailed explanations of the provisions for the protection of the network from intelligence actions by a cyber attacker.

Keywords: network reconnaissance, vulnerability, attack scenario, risk landscape private enterprise security policy.

Submitted 03.05.2023

Information about the authors

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

Grigory A. Ostapenko – Dr. Sc. (Technical), Vice-Rector of the Financial University under the Government of the Russian Federation, e-mail: alexanderostapenkoias@gmail.com

Daria V. Shcherbakova - applicant, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Alexander A. Ostapenko – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com