УДК 004.56 DOI: 10.26102/2310-6018/2020.29.2.033

Подход к анализу маршрутов сетевой атаки

И.А. Кузнецов, В.С. Оладько

Федеральное государственное бюджетное образовательное учреждение высшего образования «Финансовый университет при Правительстве Российской Федерации» Москва, Российская Федерация

Резюме: В статье затрагиваются актуальные на сегодняшний день проблемы и инструментарий анализа процессов обеспечения безопасности информации сетевой инфраструктуры. Проанализированы современные тенденции нарушений информационной безопасности в 2018-2019 годах, сделан вывод об актуальности противодействия угрозам, связанным с несанкционированным доступом к сетевым ресурсам и объектам. Проведен анализ организации типовой сетевой инфраструктуры, выделены основные элементы: субъекты, объекты и ресурсы доступа. Сделан вывод, что наиболее важными элементами с точки зрения безопасности является сетевое и серверное оборудование. Выделены основные источники угроз нарушения безопасности сети, составлена и описана цепочка реализации угрозы сетевой безопасности, показана значимость угроз источниками которых являются внешние и внутренние нарушители. Приведен пример схемы реализации сетевой атаки при эксплуатации уязвимости BDU:2017-02494. Предложен подход к построению маршрутов сетевой атаки для внутреннего и внешнего нарушителя безопасности. Показано, что маршрут сетевой атаки представляет порядок преодоления технических, а также логических устройств, содержащих меры защиты при реализации атаки на объект сетевой инфраструктуры. Разработан алгоритм построения сетевой атаки. Сделан вывод о возможности применения подхода к построению маршрута сетевой атаки в задачах мониторинга безопасности, оценки защищенности и планирования защитных мер.

Ключевые слова: уязвимость, сетевая безопасность, событие безопасности, вектор атаки, нарушитель.

Для цитирования: Кузнецов И.А., Оладько В.С. Подход к анализу маршрутов сетевой атаки. *Моделирование, оптимизация и информационные технологии.* 2020;8(2). Доступно по: https://moit.vivt.ru/wp-content/uploads/2020/05/KuznetsovOladko_2_20_1.pdf DOI: 10.26102/2310-6018/2020.29.2.033

Network attack route analysis approach

I.A. Kuznetsov, V.S. Oladko

Federal State Budgetary Educational Institution of Higher Education «Financial University under the Government of the Russian Federation» Moscow, Russian Federation

Abstract: The article discusses current problems and tools for ensuring information security in network infrastructure. The author analyzes the current trends in information security breaches in 2018-2019, concludes about the relevance of countering threats related to unauthorized access to network resources and objects. A typical network infrastructure was analyzed, the main elements were identified: subjects, objects and access resources. The most important security elements are network and server hardware. The main sources of threats to network security violations are identified, a chain of threats to network security is compiled and described, the significance of threats is shown by sources of which are external and internal violators. An example of a network attack implementation scheme during exploitation of the BDU vulnerability: 2017-02494 is given. An approach to building network attack routes for an internal and external security intruder is proposed. It is shown that the network attack route represents

the procedure for overcoming technical as well as logical devices containing security measures when implementing an attack on a network infrastructure object. An algorithm for constructing a network attack has been developed. The conclusion is drawn about the possibility of applying the approach to building a network attack route in the tasks of security monitoring, security assessment and planning of protective measures.

Keywords: vulnerability, network security, security event, attack vector, intruder.

For citation: Kuznetsov I.A., Oladko V.S. Approach to the description of network attack model route. *Modeling, Optimization and Information Technology*. 2020;8(2). Available from: https://moit.vivt.ru/wp-content/uploads/2020/05/KuznetsovOladko_2_20_1.pdf DOI: 10.26102/2310-6018/2020.29.2.033 (In Russ).

Введение

На сегодняшний день деятельность любой организации зависит от ее развития и надежности функционирования сетевой инфраструктуры, включая объекты, субъекты и ресурсы доступа. Нарушение работы сетевой инфраструктуры или несанкционированный доступ к ее ресурсам приводит к возникновению множества рисков: информационных, операционных, репутационных и финансовых. По данным аналитических отчетов компаний, занимающихся деятельностью в области информационной безопасности (ИБ) [1-3] лишь 8% организаций компаний имеют достаточный уровень защищенности сетевой инфраструктуры от внешних атак при постоянно возрастающем количестве угроз ИБ, особенно данная проблем критичная для организаций финансово-кредитной сферы. Согласно ГОСТ Р 57580.2-2018 [4] защита вычислительных сетей, предотвращение нарушения конфиденциальности информации через различные каналы утечки, управление инцидентами безопасности и и защита информации при осуществлении удаленного логического доступа с использованием устройств различного типа являются ключевыми процессами обеспечения информационной безопасности финансово-кредитных организаций, следовательно, можно сделать вывод об актуальности проведения исследований и решения теоретико-практических задач в области кибербезопасности сетевой инфраструктуры.

Объектом исследования в статье причины нарушения сетевой безопасности. Предметом исследования являются методы, алгоритмы и процедуры анализа и описания процессов реализации сетевых атак.

Целью - разработка модели и алгоритма описания вектора реализации сетевой атаки. Для достижения поставленной цели авторами решаются задачи, связанные с анализом типовой сетевой инфраструктуры, причин возникновения инцидентов сетевой безопасности и способом формализованного описания векторов атак.

Основным методами исследования при выполнении работы являлись: метод сравнения и описания, системного анализа, элементы теории множеств, а также методы теории вероятностей.

Исследованием вопросов, связанных с сетевой безопасностью занимаются такие авторы как: Шелухин О.И., Филинова А.С., Гавришев А.А., Никишова А.В., Соколов С.С., Глебов Н.Б., Марков А.В.

Проведенный анализ материалов работ данных авторов позволяет утверждать, что большинство направлений проводимых исследований связаны с совершенствованием уже существующих классических моделей оценки защищенности сетевой инфраструктуры различного типа [5,6], выявлением компьютерных атак и анализом сетевых аномалий [7-9], совершенствованием систем сетевой безопасности [10]. Однако,

в работах уделено недостаточное внимание вопросам построения маршрутов сетевых атак.

Концепция сетевой инфраструктуры

Сетевая инфраструктура - это взаимосвязанная совокупность средств приема, обработки и передачи данных, участвующая в технологических и бизнес-процессах организации, обеспечивающая субъектам доступа логический дистанционный доступ к данным, объектам и ресурсам и их коллективное использование в рамках организации (Рисунок 1).

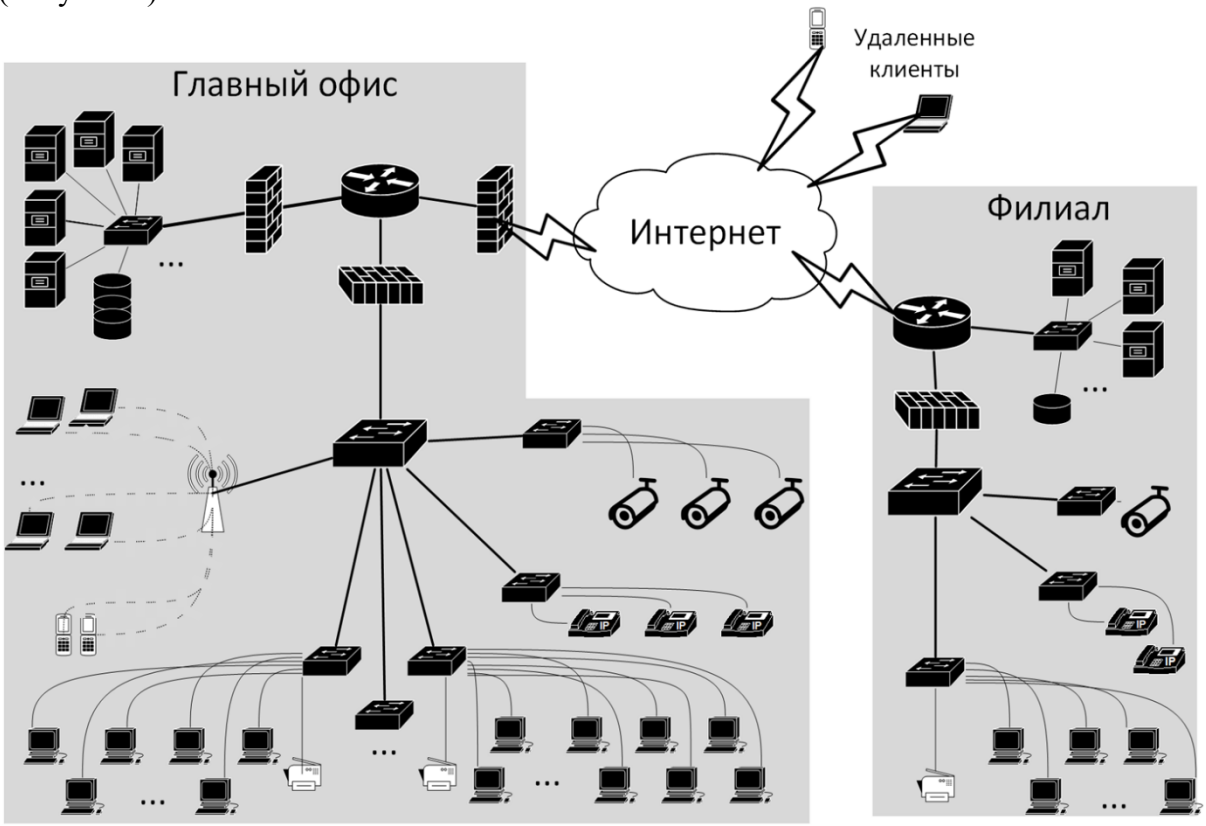

Рисунок 1. Пример типовой сетевой инфраструктуры организации
Figure 1. An example of an organization typical network infrastructure

Основная задача передающих устройств, объединение определенного количества объектов и ресурсов доступа и организация обмена информацией между ними. Необходимость высокого уровня защиты данного типа устройств обусловлена двумя факторами. Во-первых, при сбоях и поломках в работе передающего устройства возможности обмениваться информацией лишаются все подключенные к нему конечные устройства. Таким образом можно приостановить работу целого отдела сотрудников или группы сервисов. Во-вторых, при получении доступа к передающему устройству появляется возможность перехватывать информацию, исходящую от всех подключенных устройств.

Нарушение безопасности одного из элементов сетевой инфраструктуры понижает состояние защищенности всей системы. При этом, у каждого элемента сети различные функции и степени важности. Современная структура сетей построена на древовидной топологии. Это обусловлено разделением функций. Из-за такого строения сети критическими для нее становятся передающее оборудование и серверная часть. Им

необходимо повышенные меры защиты. Взаимодействие с внешней средой повышает риски возникновения угроз. Следовательно, необходим строгий контроль исходящей и входящей информации. Так же свойством любой системы является ее развитие с течением времени. Поэтому меры защиты должны своевременно обновляться исходя из перечня актуальных угроз сетевой безопасности и векторов атак.

Цепочка реализации угроз безопасности сетевой инфраструктуры

Под угрозой [11] сетевой безопасности понимается совокупность факторов и условий, создающих реальную или потенциальную опасность нарушения ИБ сетевой инфраструктуры, способные вызвать негативные последствия для организации. При анализе существующих классификаций угроз ИБ было выделено два основных класса угроз:

- угрозы, воздействующие на информацию и ресурсы доступа внутри сетевой инфраструктуры;
- угрозы, направленные на нарушение работоспособности объектов доступа сетевой инфраструктуры.

Остальные известные виды угроз являются производными от указанных выше. Формой проявления угрозы сетевой кибербезопасности является наступление одного или нескольких взаимосвязанных событий и/или инцидентов ИБ, приводящих к нарушению свойств ИБ объектов, ресурсов и субъектов доступа сетевой инфраструктуры организации. У каждой угрозы есть три общих элемента: источник, использованная уязвимость и объект, на который она направлена. Формой проявления угрозы могут быть аномалии сетевого трафика [10], события и инциденты ИБ [12]. Процесс реализации угрозы ИБ для сетевой инфраструктуры представлен на Рисунке 2.

Рисунок 2. Цепочка реализация угрозы сетевой безопасности
Figure 2. Diagram of a network security threat

Источники бывают антропогенными, техногенными и стихийными. Антропогенные источники связаны с деятельностью внутренних и внешних нарушителей кибербезопасности, действия которых могут иметь умышленный и случайный характер. Под вторым видом понимаются отказы и сбои оборудования, под третьим – непредвиденные стихийные бедствия (наводнения, землетрясения и т.д.). При грамотном построении мер защиты вероятность их появления слишком мала по

сравнении с антропогенным источником. Поэтому они не рассматриваются в исследовании.

Основными объектами атаки [6, 8] являются сетевые устройства и серверная часть сетевой инфраструктуры (Рисунок 3):

- через них передается и хранится информация, представляющая наибольшую ценность для злоумышленника (базы данных сотрудников, финансовая информация, план развития, стратегия);
- вывод из строя подобного оборудования ведет к невозможности обмена информации внутри сети и невозможности использовать сервисы, необходимые для нормального функционирования технологических и бизнес-процессов.

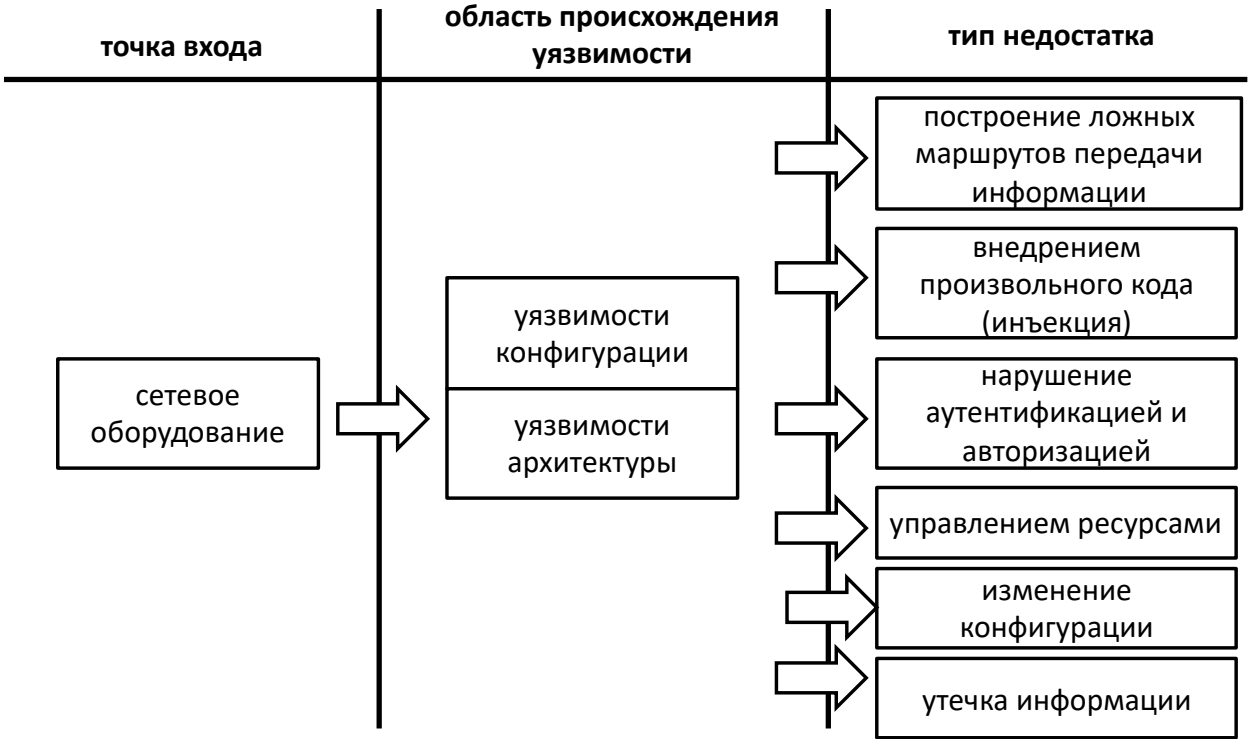

Рисунок 3. Пример сетевой атаки через уязвимость BDU:2017-02494
Figure 3. An example of a network attack through the BDU vulnerability: 2017-02494

Способы нарушения защищенного периметра у внешнего нарушителя – начало любой его атаки, он может либо найти уязвимость в межсетевом экране, либо искать беспроводную точку доступа, сигнал которой выходит за территорию контролируемой зоны (КЗ), найти инсайдера, учетную запись и права доступа которого можно использовать. Внутренний нарушитель начинает атаку внутри КЗ, начать может с любого конечного устройства или канала связи, куда не контролируется физический доступ. Межсетевой экран внутри настроен более лояльно, так как необходима эффективная работа организации, а значит более быстрый обмен информацией.

Построение маршрута сетевой атаки

Вероятность нахождения той или иной уязвимости зависит от характеристик нарушителя кибербезопасности и состава защитных мер. Последовательность действий, необходимых для получения вероятности нахождения уязвимости аналогична этапу

моделирования нарушителя. Предпочтение необходимо отдавать статистическим данным, основанных на большем количестве данных. При невозможности необходимо использовать экспертный метод.

Под маршрутом атаки понимается порядок технических, а также логических устройств, содержащих меры защиты, которые необходимо преодолеть, чтобы реализовать атаку на объект сетевой инфраструктуры.

После выбора объекта атаки и постановки цели нарушитель находит все возможные маршруты до конечного объекта. Исходя из поставленных задач и имеющихся ресурсов (технические, временные, интеллектуальные и финансовые) происходит выбор маршрута нарушителем. Сбор информации о корпоративной сети коммерческой организации возможен по ряду причин. Такая возможность обусловлена особенностями сетевых протоколов, необходимых для обнаружения отказов оборудования и обнаружения других устройств. Вторая причина — это существование специального ПО, позволяющего незаметно собирать и прослушивать входящий, исходящий и транзитный трафик.

Для реализации угрозы необходимо преодоление защитных мер на запланированном маршруте атаки. При этом не существует возможности обойти уязвимости минуя их порядок. Типовой пример — это внешний нарушитель, который хочет получить несанкционированный доступ к базе электронного документооборота с целью продать какую-либо информацию конкурентам коммерческой организации. Маршрут его атаки представлен на рисунке (Рисунок 4).

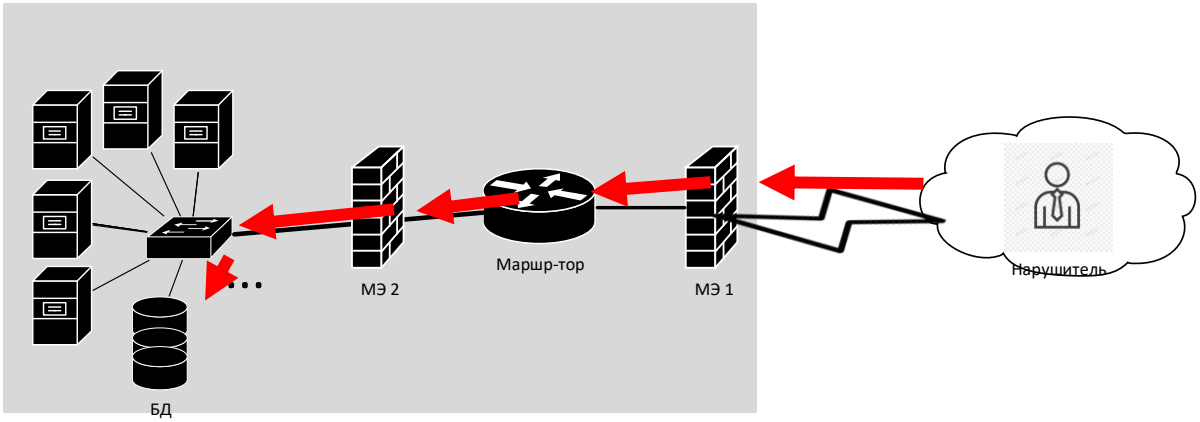

Рисунок 4. Пример атаки внешнего нарушителя кибербезопасности
Figure 4. Example cyber attacks external violator

Для успешного доступа ему необходимо вначале преодолеть первый межсетевой экран. Затем обойти правила разграничения доступа на маршрутизаторе. Потом ему следует попытаться преодолеть второй межсетевой экран прикладного уровня. Последним этапом является получение НСД к БД электронного документооборота. Чтобы преодолеть каждый из четырех этапов своей атаки, ему необходимо воспользоваться какой-либо уязвимостью из представленных ранее классов. При этом их использование имеет последовательный характер, то есть невозможно использовать уязвимости для преодоления, например, маршрутизатора, не преодолев защитную меру, которая стоит до него, а именно первый МЭ. Таким образом, события зависимы друг от друга и вероятность реализации угрозы (P) можно представить, как цепь зависимых событий (1):

$$P = \prod_i p(v_i) \quad (1)$$

Последним шагом является оценка ущерба от атаки. Она зависит от важности объекта атаки и типа угрозы. Самыми критичными элементами в корпоративной сети являются – сетевое оборудование и сервер. В устройстве корпоративной сети может быть несколько коммутаторов и маршрутизаторов, а также могут быть настроены резервные маршруты информации. На важность сетевого оборудования влияют такие показатели как:

- количество подключенных устройств;
- проходит ли через него маршрут информации во внешнюю сеть;
- проходит ли маршрут информации до сервера.

Ущерб от атак на каналы связи зависит от количества трафика и его важности. Важность серверного оборудования обуславливается наличием серверной части всех клиент-серверных приложений, а также сетевых сервисов, таких как электронная почта или ip-телефония. Количество установленных приложений и сетевых сервисов прямо пропорционально влияет на размер ущерба при реализации атаки.

Результаты

Ущерб от реализации атаки нарушителем зависит от структуры корпоративной сети, и в каждом случае оценка будет уникальной. Но ущерб от реализации угрозы при атаке на такие объекты как сервер или центральный маршрутизатор должен оцениваться как максимальный. При атаках на другие объекты оценка потенциального ущерба должна быть ниже.

Алгоритм действий при оценке маршрутов проведения нарушителем сетевой атаки представлен на Рисунке 5.

Промежуточным выводом является понимание, что внешний нарушитель находится вне корпоративной сети, а потенциальный внутренний – не проявляется до момента начала атаки. Поэтому служба ИБ организации с помощью мер защиты не может повлиять на параметры нарушителя, а только оценить их. Повышение оценки защищенности возможно только воздействием на следующие параметры:

- вероятности использования уязвимости нарушителем;
- потенциальный ущерб.

Заключение

Ключевыми элементами процесса реализации угрозы сетевой безопасности являются: нарушитель, уязвимость и объект атаки. Построение модели нарушителя кибербезопасности и детальное описание множеств уязвимостей должны быть неотъемлемыми процессами методики оценки соответствия защитных мер требованиям безопасности.

Модель нарушителя строится из показателей трех параметров, где каждый показатель обладает двумя характеристиками: вероятность появления и относительная степень ущерба. Для каждого из них можно найти статистику в открытых источниках, что повышает степень объективности данной модели. При необходимости, данные статистические показатели можно уточнить с помощью экспертного метода или анализом данных при работе организации.

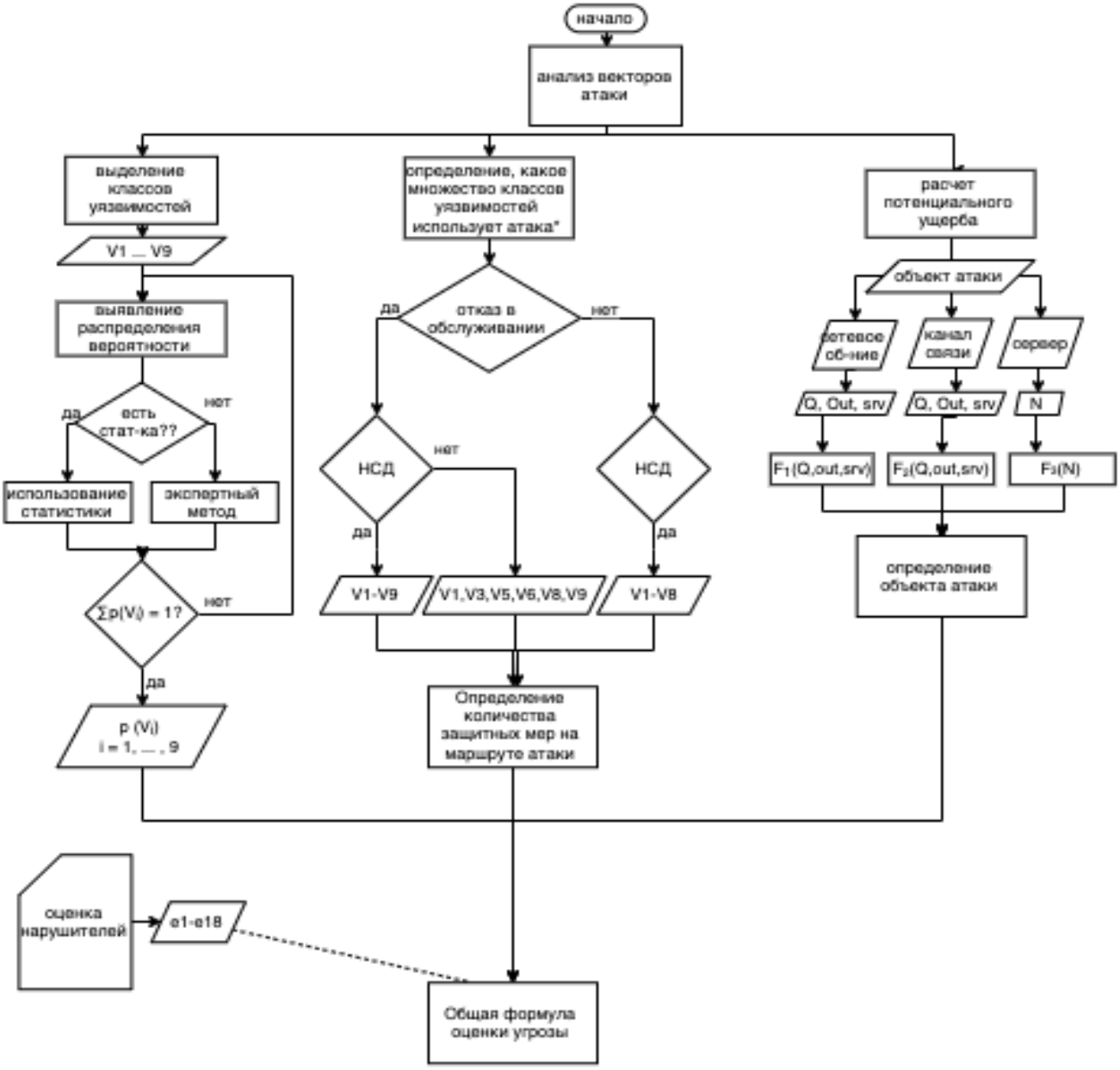

Рисунок 5. Алгоритм действий при анализе маршрутов атаки
Figure 5. Attack route analysis algorithm

При составлении структуры мер защиты важным параметром являются предполагаемые маршруты атаки нарушителем. Их необходимо строить из предположения, что нарушитель хочет максимально реализовать свои возможности и нанести наибольший ущерб. Таким образом, защитные меры должны быть выстроены по концепции многоуровневой защиты, где центральными элементами являются сервер и сетевое оборудование. Разработанный алгоритм и концепция построения маршрутов атаки нарушителя на сетевую инфраструктуру организации может быть использованы при планировании мер защиты, моделировании систем ИБ, как элемент входных данных системы принятия решений [13].

ЛИТЕРАТУРА

1. Аналитический отчет компании «Positive technologies»: Уязвимости корпоративных информационных систем, 2019. Доступно по адресу: https://www.ptsecurity.com/ru-ru/research/analytics/corporate-vulnerabilities-2019/ (дата обращения: 05.02.2020).
2. Сборник исследований по практической безопасности «Positive Research 2018». Доступно по адресу: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Positive-Research-2018-rus.pdf (дата обращения: 02.02.2020).
3. Аналитический отчет ГК «Infowatch»: Актуальные киберугрозы — 2018. Тренды и прогнозы. Доступно по адресу: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018/ (дата обращения: 17.02.2020).
4. ГОСТ Р 57580.2-2018 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия. Доступно по адресу: http://docs.cntd.ru/document/1200158801
5. Гавришев А.А. Обобщенный вычислительный метод сравнения точности количественный оценок защищенности беспроводных систем безопасности. *Моделирование, оптимизация и информационные технологии.* 2019;7(3). Доступно по: http://moit.vivt.ru/ DOI:10.26102/2310-6018/2019.26.3.002 (дата обращения: 02.02.2020).
6. Марков А.В. Модель угроз безопасности информации в локальных корпоративных сетях. *REDS: Телекоммуникационные устройства и системы*. 2016;4:580-583.
7. Шелухин О.И. Обнаружение сетевых аномальных выбросов трафика методом разладки Бродского-Дарховского/ Шелухин О.И., Филинова А.С. *T-Comm - Телекоммуникации и Транспорт*. 2013;7(10):116-118.
8. Соколов С.С. Современные методы социальной инженерии - пути реализации угроз безопасности корпоративных сетей передачи данных/ Соколов С.С., Глебов Н.Б. *Региональная информатика и информационная безопасность. - СПб.: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления*. 2016.
9. Конарев И.И. Анализ методов обнаружения атак на WI-FI / Конарев И.И., Никишова А.В. *Актуальные вопросы информационной безопасности регионов в условиях перехода России к цифровой экономике материалы VII Всероссийской научно-практической конференции. Волгоградский государственный университет*. 2018:28-32.
10. Бабенко А.А. Разработка системы управления аномальными событиями информационной безопасности/ Бабенко А.А., Микова С.Ю., Оладько В.С. *Информационные системы и технологии*. 2017;5(103):108-116.
11. Национальный стандарт Российской Федерации ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. Доступно по: http://docs.cntd.ru/document/1200123702 (дата обращения: 12.02.2020)
12. Оладько В.С. Инциденты сетевой безопасности в системе цифровой экономики. *Научный результат. Информационные технологии.* 2019;4(4):19-30. DOI: 10.18413/2518-1092-2019-4-4-0-3. (дата обращения: 12.02.2020)
13. Витенбург Е.А. Принятие решений на основе данных мониторинга информационных систем предприятий/ Витенбург Е.А., Никишова А.В., Оладько В.С., Умницын М.Ю., Омельченко Т.А., Садовникова Н.П. *Управление развитием крупномасштабных систем MLSD'2019 Материалы двенадцатой международной конференции Научное электронное издание. Под общей ред. С.Н. Васильева, А.Д. Цвиркуна*. 2019:1031-1033. DOI: 10.25728/mlsd.2019.1.1031

REFERENCES

1. Analiticheskiy otchet kompanii «Positive technologies»: Uyazvimosti korporativnykh informatsionnykh sistem, 2019. Available at: https://www.ptsecurity.com/ru-ru/research/analytics/corporate-vulnerabilities-2019/ (accessed: 05.02.2020).
2. Sbornik issledovaniy po prakticheskoy bezopasnosti «Positive Research 2018». Available at: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Positive-Research-2018-rus.pdf (accessed: 02.02.2020).
3. Analiticheskiy otchet GK «Infowatch»: Aktual'nyye kiberugrozy — 2018. Trendy i prognozy. Available at: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018/ (accessed: 17.02.2020).
4. GOST R 57580.2-2018 Bezopasnost finansovykh (bankovskikh) operatsiy. Zashchita informatsii finansovykh organizatsiy. Metodika otsenki sootvetstviya. Available at: http://docs.cntd.ru/document/1200158801 (accessed: 02.02.2020). (In Russ)
5. Gavrishev A.A. Generalized computational method to compare the accuracy of quantitative estimates of security f wireless security systems. *Modeling, Optimization and Information Technology*. 2019;7(3). Available at: http://moit.vivt.ru/ DOI:10.26102/2310-6018/2019.26.3. (In Russ)
6. Markov A.V. Model ugroz bezopasnosti informatsii v lokalnykh korporativnykh setyakh. *REDS: Telecommunication devices and systems*. 2016;4:580-583. (In Russ)
7. Sheluhin O.I., Filinova A.S. Detection of network anomaly bursts of traffic by the method of the disorder of Brodsky- Darkhovsky. *T-Comm - Telecommunications and Transport.* 2013;7(10):116-118. (In Russ)
8. Sokolov S.S., Glebov N.B. Modern methods of social engineering - ways of implementing threats to the security of corporate data transmission networks. *Regional informatics and information security. - SPb.: St. Petersburg Society of Informatics, Computer Engineering, Communication and Control Systems*. 2016:130-132. (In Russ).
9. Konarev I.I., Nikishova A.V. Analiz metodov obnaruzheniya atak na WI-FI. *Aktual'nyye voprosy informatsionnoy bezopasnosti regionov v usloviyakh perekhoda Rossii k tsifrovoy ekonomike materialy VII Vserossiyskoy nauchno-prakticheskoy konferentsii. Volgogradskiy gosudarstvennyy universitet*. 2018. (In Russ)
10. Babenko A.A., Mikova S.Yu., Oladko V.S. Development of information security abnormal events control system. *Informatsionnyye sistemy i tekhnologii.* 2017;5(103):108-116. (In Russ).
11. Natsional'nyy standart Rossiyskoy Federatsii GOST R 56546-2015 Zashchita informatsii. Uyazvimosti informatsionnykh sistem. Klassifikatsiya uyazvimostey informatsionnykh sistem. Available at: http://docs.cntd.ru/document/1200123702 (accessed: 12.02.2020) (In Russ).
12. Oladko V.S. Network security incidents in the digital economy system. *Research result.* 2019; 4(4): 19-30. DOI: 10.18413/2518-1092-2019-4-4-0-3. (In Russ).
13. Vitenburg Y.A., Nikishova A.V., Oladko V.S., Umnitsyn M.Yu., Omelchenko T.A., Sadovnikova N.P. Prinyatiye resheniy na osnove dannykh monitoringa informatsionnykh sistem predpriyatiy. *Upravleniye razvitiyem krupnomasshtabnykh sistem MLSD'2019 Materialy dvenadtsatoy mezhdunarodnoy konferentsii Nauchnoye elektronnoye izdaniye. Pod obshchey red. S.N. Vasil'yeva, A.D. Tsvirkuna.* 2019:1031-1033. DOI: 10.25728/mlsd.2019.1.1031/ (In Russ).

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Кузнецов Иван Александрович, магистр, кафедра информационной безопасности, ФГБОУ ВО "Финансовый университет при Правительстве Российской Федерации", Москва, Российская Федерация.

Оладько Владлена Сергеевна, к-т. техн.. наук, доцент, кафедра информационной безопасности, ФГБОУ ВО "Финансовый университет при Правительстве Российской Федерации", Москва, Российская Федерация.
e-mail: vsoladco@fa.ru
ORCID: 0000-0003-0500-8928

Ivan A. Kuznetsov, Magistrate, Information Security Department, Federal State Budget Educational Institution Of Higher Education "Financial University Under The Government Of The Russian Federation ", Moscow, Russian Federation

Vladlena S. Oladko, Cn. Sci. (Technical), Assistant Professor, Information Security Department, Federal State Budget Educational Institution Of Higher Education "Financial University Under The Government Of The Russian Federation ", Moscow, Russian Federation
E-Mail: Vsoladco@Fa.Ru
ORCID: 0000-0003-0500-8928