УКД 004.7

***Д.И. Воронин, Д.В. Кочкин***
*Вологодский государственный университет*

# СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПО ВОПРОСАМ БЕЗОПАСНОСТИ КОМПЬЮТЕРНОЙ СЕТИ

В статье рассмотрены результаты исследования в области систем поддержки принятия решения в компьютерных сетях. Представлена система поддержки принятия решений по вопросам безопасности компьютерной сети. Определены методы внедрения данной системы в структуру корпоративной сети. Проведен анализ применимости системы поддержки принятия решений и порядок эксплуатации.

Система поддержки принятия решений, информационная безопасность, кибербезопасность, компьютерные сети, модель угроз.

Каждую секунду через каналы связи компьютерных сетей проходит огромное количество информации [1, 2]. Наряду с обеспечением качественного обмена информацией важным вопросом также является обеспечение сетевой безопасности от различных угроз.

Злоумышленники взламывают системы по разным причинам и с разными целями. Поэтому важно понимать, как они атакуют и эксплуатируют эти системы, а также вероятные причины этих атак.

Системные администраторы и специалисты по безопасности должны защищать свою инфраструктуру от эксплойтов, зная врагов, которые стремятся использовать ту же инфраструктуру для незаконных действий.

Злоумышленники преследуют множество различных целей для взлома информационных систем. Ключом для эффективного противодействия злоумышленникам является понимание используемых методов для осуществления кибератак. Единственное, что объединяет как системных администраторов, специалистов по безопасности, так и злонамеренных хакеров, – инфраструктура, различаются лишь цели ее использования.

Основными аспектами информационной безопасности является защита информации и информационных систем от несанкционированного доступа, раскрытия, изменения и уничтожения информации. Злонамеренные действия хакеров могут привести к огромным финансовым потерям, повлиять на репутацию организации и пользователей.

За каждым взломом информационной системы стоит определенный мотив. Мотив возникает, когда информационная система хранит в себе что-то ценное для злоумышленника. Цель, как правило, одна – получить некую выгоду, нарушить работоспособность организации, украсть ценную информацию, повлиять на репутацию компании или ее экономику. В настоящее время существуют также политические и военные мотивы. Злоумышленники вмешиваются в политические и военные процессы государства и прикладывают усилия, чтобы пошатнуть безопасность государства и повлиять на его суверенитет. Существует множество различных инструментов для достижения этих целей. Задачей государства является противодействие кибератакам.

Кибератаки включают в себя совокупность мотива, метода и уязвимости. Основные мотивы, стоящие за атаками на информационную безопасность, следующие:

- нарушение непрерывности бизнеса, которое влечет за собой экономические убытки и потерю репутации компании;
- кража информации для последующего распространения и использования ее для незаконных действий. Например, продажа персональных данных третьим лицам;
- влияние на производственные процессы может повлечь за собой тяжкие последствия. Например, нарушение работы электростанций;
- с помощью влияния на средства массовой информации можно пропагандировать религиозные или политические убеждения;
- участие в кибервойнах способствует достижению военных целей государства;
- мошенничество и шантаж, требование выкупа также являются одним из основных мотивов злоумышленников.

Кибератаки подразделяются на пять основных категорий: пассивные, активные, проникающие, инсайдерские и распределенные.

Существуют методы и инструменты проведения пассивных кибератак. Эти атаки очень трудно обнаружить, потому что не происходит активного взаимодействия с компьютерной сетью. Злоумышленник производит разведку архитектуры компьютерной се-

ти. Для этого проводится мониторинг и перехват сетевого трафика для дальнейшего анализа с помощью снифферов.

Используя методы пассивной атаки, злоумышленник может перехватить незашифрованные данные, учетные данные и конфиденциальную информацию, которую можно использовать в дальнейшем при проведении активных атак.

Примеры пассивных атак:

• отслеживание и прослушивание информации;

• анализ сетевых данных;

• расшифровка слабо зашифрованных данных.

Активные атаки воздействуют на передаваемые данные или нарушают обмен данными с целью обхода или взлома защищенных систем. Злоумышленники запускают атаки на целевую систему или сеть, отправляя специальные действия, которые могут быть обнаружены. Эти атаки выполняются в целевой сети с целью использования передаваемой информации. Они проникают во внутреннюю сеть цели или заражают ее, получая доступ к удаленной системе для компрометации внутренней сети.

Примеры активных атак:

• атака типа «отказ в обслуживании» (DoS);

• обход защитных механизмов;

• атаки вредоносных программ (таких как вирусы, черви, программы-вымогатели);

• изменение информации;

• подмена информации;

• повторные атаки;

• атаки на основе пароля;

• перехват сеанса;

• атака «Человек по середине»;

• заражение DNS и ARP;

• атака с использованием скомпрометированного ключа;

• атака брандмауэром и IDS;

• атака на профиль;

• выполнение произвольного кода;

• повышение привилегий;

• доступ через Backdoor;

• криптографические атаки;

• SQL-инъекция;

• атаки XSS;

• атаки на обход каталогов;

• использование уязвимостей прикладного программного обеспечения и операционной системы.

Проникающие атаки выполняются в непосредственной близости от компьютерной сети. Целью такой атаки является сбор, изменение информации или нарушение доступа к ней. Для этого злоумышленники используют учетные данные. К проникающим атакам относится социальная инженерия.

Инсайдерские атаки выполняются лицами, имеющими физический и приватный доступ к инфраструктуре. Целью является получение доступа к конфиденциальной информации, возможностью повлиять на целостность и доступность информационной системы.

Примеры инсайдерских атак:

• прослушивание и повторное использование Wi-Fi;

• кража физических устройств;

• социальная инженерия;

• кража данных;

• использование капсул;

• установка кейлоггеров, бэкдоров или вредоносного ПО.

Стоит отметить, что атаки с близкого расстояния и инсайдерские атаки трудно распознать. Задачей специалистов в области администрирования и обеспечения безопасности компьютерных сетей является наличие компетенций по способам противодействия и защиты информации от кибератак.

Распределенные атаки происходят, когда злоумышленники вмешиваются в аппаратное или программное обеспечение у его источника или когда оно находится в эксплуатации. Примеры таких атак включают бэкдоры, созданные поставщиками программного обеспечения или оборудования на этапе производства. Злоумышленники используют эти бэкдоры для получения несанкционированного доступа к целевому информационному ресурсу, системам или сети.

Примеры распределенных атак:

• модификация программного или аппаратного обеспечения во время выпуска продукта;

• модификация программного или аппаратного обеспечения во время распространения.

Информационная безопасность должна снижать возможность кражи, подделки или нарушения работы информации и услуг до низкого или допустимого уровня. Обладатель информации обязан принимать меры по защите информации согласно законодательству РФ, в котором указаны требования к построению системы защиты информации, а также требования к мониторингу информационной безопасности и уведомлению об инцидентах.

Существует множество источников и баз данных, которые содержат информацию о наиболее распространенных векторах развития компьютерных атак [3, 4]. Например, MITRE ATT&CK, OWASP Top 10, CAPEC, WASC и др.

Понимание тактики злоумышленника помогает прогнозировать и обнаруживать возникающие угрозы на ранних стадиях. Понимание способов реализации угроз, используемых злоумышленниками, помогает выявить уязвимости и заранее принять защитные меры. Наконец, анализ техник, используемых злоумышленниками, помогает определить, что злоумышленник ищет в инфраструктуре целевой организации.

Чтобы защитить свою сеть от злоумышленников и предстоящих атак необходимо останавливать атаки на начальном этапе, тем самым защищая сеть от масштабных повреждений. Специалисты по безопасности должны осуществлять непрерывный мониторинг индикаторов компрометации, чтобы эффективно обнаруживать новые киберугрозы и реагировать на них.

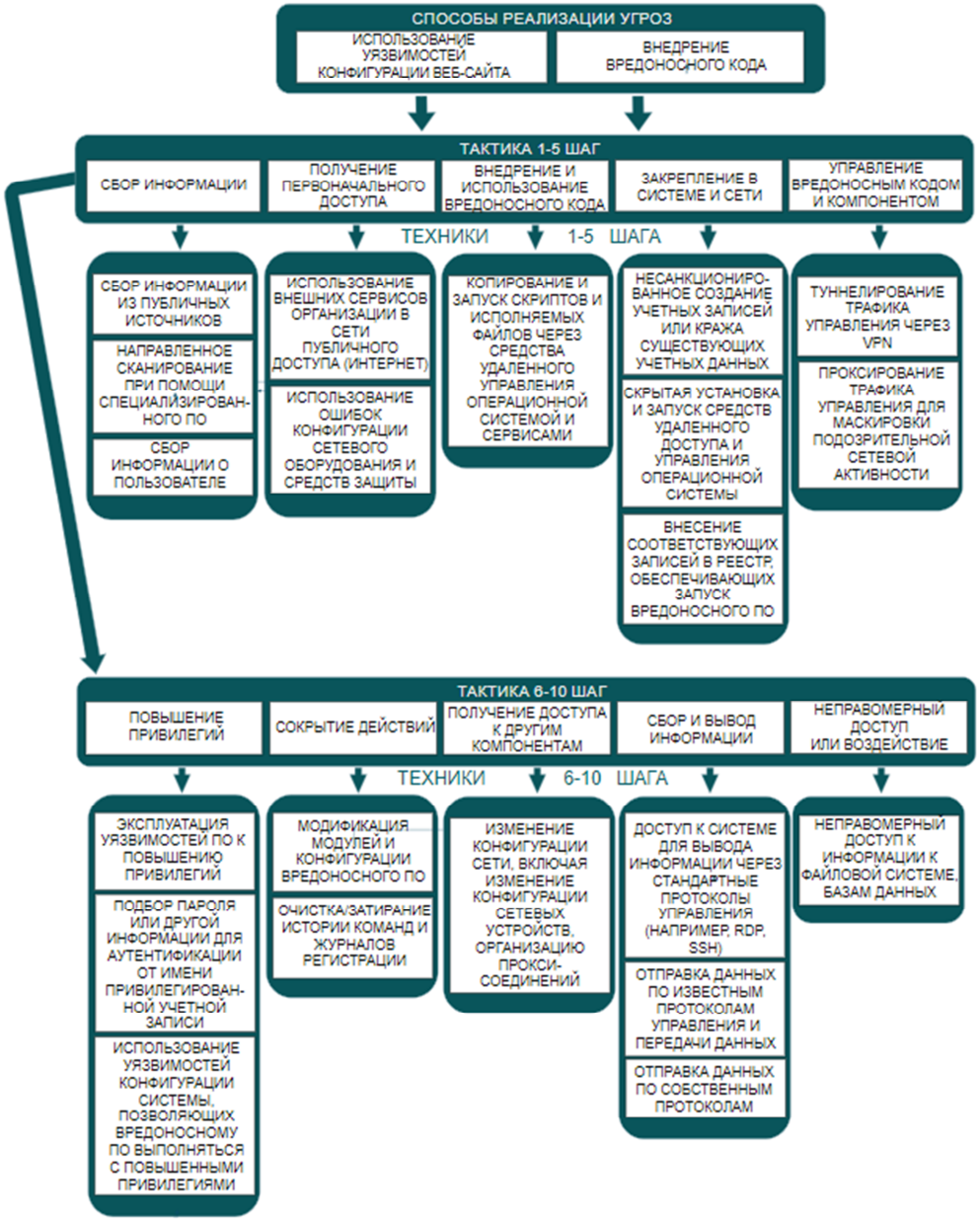


*Рис. 1. Сценарий несанкционированного доступа к базам данных*

Ключевыми индикаторами компрометации являются: необычный исходящий сетевой трафик, необычная активность через привилегированную учетную запись пользователя, географические аномалии, несколько неудачных попыток входа, увеличенный объем чтения базы данных, большой размер HTML-ответа, несколько запросов на один и тот же файл, несовпадающий трафик порта приложения, подозрительные изменения реестра или системных файлов, необычные DNS-запросы, неожиданные изменения настроек систем, признаки активности распределенного отказа в обслуживании (DDoS), веб-трафик с нестандартным поведением.

На рисунке 1 показан сценарий реализации угрозы несанкционированного доступа к базам данных.

При эксплуатации компьютерных сетей необходимо определить все сценарии для каждой из существующих угроз безопасности информации. Количество таких сценариев зависит от актуального профессионального уровня нарушителей, инвентаризации компьютерных сетей, анализа уязвимостей и тестирования на проникновение.

Типовые способы удаленных атак в Internet показаны на рисунке 2.


*Рис. 2. Типовые способы удаленных атак в Internet*

Оценка угроз безопасности информации включает следующие этапы:

1) определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации;

2) определение возможных объектов воздействия угроз безопасности информации;

3) оценка возможности реализации (возникновения) угроз безопасности информации и определение их актуальности.

Общая схема оценки угроз безопасности информации приведена на рисунке 3.


*Рис. 3. Общая схема оценки угроз безопасности информации*

Как правило, управление компьютерными сетями выполняет администратор. От качества его работы зависят все процессы, происходящие внутри сети, а также все жизненные процессы человека, основанные на использовании информационных технологий. В настоящее время практически все сферы жизни человека связаны с процессом обмена информации через компьютерную сеть. Поэтому работоспособность компьютерных сетей должна обеспечивать надежность и отказоустойчивость всех сервисов и услуг, используемых человеком [5].

Огромное влияние на процесс эксплуатации компьютерных сетей оказывает человеческий фактор, до 90 % проблем в сетях вызваны действиями людей.

Двумя важными факторами сетевой безопасности являются создание всеобъемлющих политик безопасности и отображение топологии сети предприятия. К сожалению, оба эти фактора отнимают много времени. Поэтому администраторы используют искусственный интеллект для улучшения этой операции. Он может выполнять анализ сетевого трафика и по умолчанию предлагать эффективные политики безопасности.

Универсальные решения часто работают хуже специфических. Также проблемы могут повторяться, несмотря на их решение. Для поддержания работоспособности компьютерных сетей администратору необходимы инструменты, улучшающие процессы решения возникших проблем в сети. Система поддержки принятия решений (СППР) по вопросам безопасности компьютерной сети является эффективным инструментом для этой цели [6].

СППР по вопросам безопасности компьютерной сети позволяет накапливать полученные знания и опыт решения вопросов безопасности при эксплуатации компьютерных сетей, анализировать полученные данные и предлагать оптимальные решения.

Структура СППР по вопросам безопасности компьютерной сети показана на рисунке 4.


*Рис. 4. Структура СППР по вопросам безопасности компьютерной сети*

Важным вопросом является место установки СППР в компьютерной сети [7, 8]. От этого зависит количество и достоверность пакетов, переданных для анализа. Эффективным способом будет установка TAP-устройства на физическом линке в сторону пограничного маршрутизатора. Это позволит снять 100 % копию трафика из компьютерной сети.

Расположение СППР по вопросам безопасности компьютерной сети показано на рисунке 5.

В заключении можно отметить, что использование СППР по вопросам безопасности компьютерной сети повысит эффективность эксплуатации этой сети. Для опытных администраторов СППР станет удобным инструментом оптимизации и автоматизации своей работы, а для новых сотрудников – источником готовых решений.

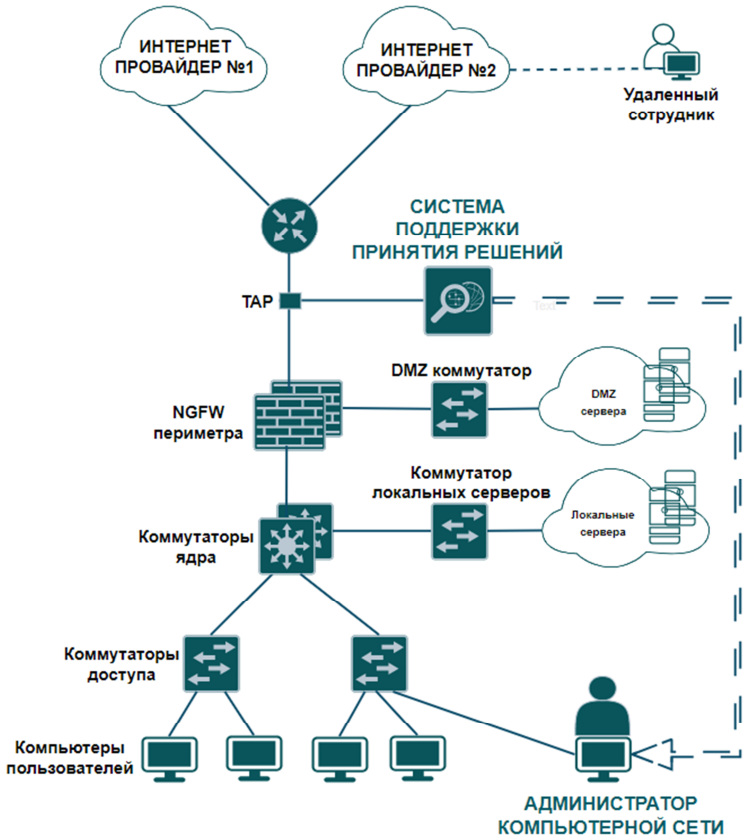


*Рис. 5. Расположение СППР в компьютерной сети*

**Литература**

1. Модели и методы построения нейро-нечетких интеллектуальных агентов в информационно-телекоммуникационных системах / А. А. Суконщиков, И. А. Андрианов, С. В. Дианов [и др.]. – Курск : Закрытое акционерное общество «Университетская книга», 2021. – 152 с. – EDN UTIOMM.

2. Интеллектуальные информационно-телекоммуникационные системы / А. Н. Швецов, А. А. Суконщиков, И. А. Андрианов [и др.]. – Вологда : Вологодский государственный университет, 2023. – 127 с. – EDN WYSWVA.

3. Методика оценки угроз безопасности информации. – URL: https://fstec.ru/files/495/---5--2021-/891/---5--2021-.pdf (дата обращения: 31.10.2024). – Текст : электронный.

4. Матрица MITRE ATT&CK. – URL: https://mitre.ptsecurity.com/ru-RU (дата обращения: 31.10.2024). – Текст : электронный.

5. Кочкин, Д. В. Моделирование информационно-телекоммуникационной системы предприятия раскрашенными сетями Петри / Д. В. Кочкин, В. А. Горбунов // Вестник Череповецкого государственного университета. – 2024. – № 1(118). – С. 48–58. – DOI 10.23859/1994-0637-2024-1-118-3. – EDN HPJRAM.

6. Принципы построения самоорганизующихся информационно-телекоммуникационных систем / А. А. Суконщиков, А. Н. Швецов, И. А. Андрианов, Д. В. Кочкин // Вестник Череповецкого государственного университета. – 2021. – № 1(100). – С. 56–67. – DOI 10.23859/1994-0637-2021-1-100-4. – EDN FUTTMS.

7. Ситуационные интеллектуальные системы поддержки принятия решений / А. Н. Швецов, А. А. Суконщиков, Д. В. Кочкин, И. А. Андрианов. – Курск : Закрытое акционерное общество «Университетская книга», 2018. – 251 с. – EDN OSGGJV.

8. Распределенные интеллектуальные информационные системы и среды / А. Н. Швецов, А. А. Суконщиков, Д. В. Кочкин [и др.] ; под редакцией А. Н. Швецова и А. А. Суконщикова. – Курск : Закрытое акционерное общество «Университетская книга», 2017. – 197 с. – EDN YNAOSP.

***D.I. Voronin, D.V. Kochkin***
*Vologda State University*

**COMPUTER NETWORK SECURITY DECISION SUPPORT SYSTEM**

The article discusses the results of the research in the field of decision support systems in computer networks. A decision support system for computer network security issues is presented, and methods for implementing this system into the corporate network structure are defined. The analysis of the applicability of the decision support system and the operating procedure is carried out.

Decision support system, information security, cybersecurity, computer networks, threat model.