Модель воздействия компьютерных атак на информационно-телекоммуникационную сеть

Лаута Олег Сергеевич
доктор технических наук, профессор, Государственный университет морского и речного флота им. адмирала С.О. Макарова, г. Санкт-Петербург, Россия, laos-82@yandex.ru

Иванов Денис Александрович
кандидат технических наук, преподаватель филиала Военно-воздушной академии им. профессора Н.Е. Жуковского и Ю.А. Гагарина, г. Челябинск, Россия, prosto_deniss@mail.ru

Аведян Эдуард Вартеванович
кандидат технических наук, доцент филиала Военно-воздушной академии им. профессора Н.Е. Жуковского и Ю.А. Гагарина, г. Челябинск, Россия, avEddoV@mail.ru

АННОТАЦИЯ

Введение: В работе представлен новый подход к классификации компьютерных атак на критически важные объекты инфраструктуры, который учитывает от комплексного изучения объекта воздействия до реализации атаки. **Постановка задачи:** к числу наиболее заметно нарастающих угроз информационной безопасности критически важного объекта инфраструктуры относятся компьютерные атаки на информационно-телекоммуникационные сети, которые являются его ключевым активом. Современные направленные компьютерных атак представляют собой сложное комплексное воздействие на сеть, в результате которого контроль ресурсов, взлом и заражение информационно-телекоммуникационных сетей. Зачастую этому предшествует долгая и кропотливая работа в киберпространстве: разведка, поиск характерных уязвимостей и захват информационных активов. Меняющийся ландшафт угроз, частота их появления, сложность и целевой характер атак – все это требует эволюции существующей парадигмы в сфере правил информационной безопасности. **Методы**: метод проведения атак; метод прогнозирования и профилирования компьютерных атак; метод анализа логической топологии сети; метод скрытых марковских моделей. **Результаты**: модель представляет собой систематизированный перечень компьютерных атак, воздействующих как на программное обеспечение элементов информационно-телекоммуникационной сети, спецификой их применения и особенностями реализации компьютерных атак, так и на субэлементы. **Практическая значимость**: Перечень угроз информационно-телекоммуникационной сети, позволяет определить опасность, а также угрозу для каждого элемента сети.

КЛЮЧЕВЫЕ СЛОВА: критически важный объект инфраструктуры; информационная система; классификация; классификатор; информационно-телекоммуникационная сеть; компьютерная сеть; защита информации; киберпространство; компьютерная атака; сетевое устройство.

Введение

Современный этап развития общества характеризуется повышением роли информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры и субъектов, осуществляющих сбор, формирование, распространение и использование информации. Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, которые определяются целостностью сбалансированных интересов личности, общества и государства. К числу наиболее заметно нарастающих угроз информационной безопасности критически важного объекта инфраструктуры относятся компьютерные атаки (КА) на информационно-телекоммуникационные сети (ИТКС), которые являются его ключевым активом.

Количество КА на объекты критически важной инфраструктуры в 2019 г. по сравнению с 2012 г. увеличилось более чем в два раза

Современные направленные КА представляют собой сложное комплексное воздействие на сеть, в результате которого контроль ресурсов, взлом и заражение ИТКС не происходят «вдруг из ничего». Зачастую этому предшествует долгая и кропотливая работа в киберпространстве: разведка, поиск характерных уязвимостей и захват информационных активов [1]. Меняющийся ландшафт угроз, частота их появления, сложность и целевой характер атак – все это требует эволюции существующей парадигмы в сфере правил информационной безопасности.

Для минимизации потенциального ущерба важен переход к сочетанию технологий предотвращения, обнаружения и реагирования на КА, однако сегодня анализ инцидента происходит в основном «по факту», путем «латания дыр» в уязвимостях систем обеспечения информационной безопасности [2]. Большинство государственных и частных организаций имеют средства для обнаружения известных атак, хотя, как показывает практика, данные решения не всегда спасают их от злонамеренных сетевых вторжений. Самое сложное в деле защиты конфиденциальных информационных ресурсов – это остановить неизвестные атаки, специально созданные с целью обхода имеющейся защиты, использующие изменения сигнатур и шаблонов поведения. Неотъемлемой частью аналитической работы по защите ИТКС является разработка наиболее полной классификации КА, создающих угрозы для информационных ресурсов.

Анализ решений по классификации ка

Многие известные решения по классификации компьютерных атак опираются на определенные требования, такие как:

взаимоисключаемость – категории классификации не должны пересекаться и иметь схожие значения;

исчерпываемость – классификация должна в полной мере раскрывать описываемую область исследования, максимально охватывать характеристики рассматриваемой КА;

понятность – однозначность и краткость представляемой информации;

недвусмысленность – строгое разделение представленных категорий с четко выраженной принадлежностью КА соответствующему классификатору;

полезность – возможность использования в области информационной безопасности обобщенных классификатором данных о той или иной КА;

приемлемость – построение классификации на основе анализа существующей классификации в области исследования.

Известные исследования в области классификации КА можно разделить на две крупные группы. Первая охватывает разработку общих классификаций по компьютерным атакам, основанных на типе атаки или понесенном ущербе. Вторая группа работ изучает определенные компьютерные атаки, давая наиболее глубокое представление о конкретной КА, используемых ею уязвимостях, эксплойтах и, как правило, последствиях вторжения в информационную систему (ИС) [2].

В общих классификациях акцент делается либо на разделение КА по методам проведения атак [3,4,5,6,7,8], либо на градацию по возможным потерям информационных активов в результате атаки [9,10,11].

В работе [3] проводится анализ известных классификаций компьютерных атак и представлены классификации по следующим признакам: цель, тип, модель OSI, операционная система (и ее характерные уязвимости), местоположение атакующего, тип ИС, атакуемый сервис, концентрация атаки, наличие обратной связи, условие реализации КА, тип воздействия, автоматизация, источник и количество соединений. Недостатками представленной классификации являются отсутствие определений классификаторов и недостаточное внимание к характеристикам точки воздействия, т.е. к тому, на какие ключевые узлы ИС действует та или иная КА.

В [11] приводится более 20 основных типов кибератак, используемых для внедрения в информационные ресурсы энергосистем; они разделены на четыре базовые категории. Рассматриваются математические модели для каждой категории, классификация предназначена в первую очередь для инженерного персонала, обеспечивающего системы безопасности современных критически важных объектов инфраструктуры для ИС энергетического сектора.

В работах [12,13,14,15] авторы руководствуются пятью основными классификаторами: определение природы и сущности КА, цели, воздействия КА на защищаемый информационный ресурс и мероприятиями по предотвращению угроз и их последствий. Отличительной особенностью представляемого классификатора является расширенное, многогранное описание смешанных составных сетевых атак.

Неординарный классификационный подход демонстрируют специалисты Тунисского департамента информатики [16], предложившие гибридную пятимерную модель угроз ИС, которая, во-первых, сочетает в себе классификационные методы, основанные и на технике атак, и на воздействии угроз, и, во-вторых, затрагивает возможные источники реализации угрозы, тип, мотивацию, замысел нарушителя и тип воздействия.

В работе [17] рассматриваются наиболее распространенные КА по обширному набору классификаторов и предлагаются онтологические основы для представления классификации: она отвечает требованиям полезности, взаимоисключения пунктов классификатора, понятности информации и однозначности. Однако работа [17] сосредоточена преимущественно на формализации описания сетевых КА, особенностей их подготовки и проведения.

В [18] предложена классификация методов прогнозирования и профилирования КА, таких как метод анализа логической топологии сети, метод скрытых марковских моделей, методах, основанных на нечеткой логике, методах на базе графиков сетевых атак и статистических методах анализа событий. Несмотря на многочисленный набор классификационных признаков, выделенные категории не рассматривают такие важные аспекты, как уровень

эталонной модели взаимодействия открытых систем (ЭМВОС), сетевые устройства, подвергаемые воздействию в первую очередь, а также временные характеристики КА.

Классификация атак, которая может быть использована для идентификации возможных вторжений в специализированные системы мониторинга и управления данными, приведена в [19], так и в работе в [20]. Классификаторы идентифицируют атаки на основные узлы сетевого оборудования, атаки на программное обеспечение и атаки на стеки протоколов связи, выделенные отдельно в специфике SCADA-систем, т.е. в области применения диспетчерского контроля, управления и сбора данных.

Статьи [21,22,23] рассматривают классификационные признаки КА, как параметры для глубокого машинного обучения систем защиты информационных систем, базирующихся на алгоритмах искусственных нейронных сетей.

Таким образом, анализ известных работ в области классификации компьютерных атак позволяет сделать следующие выводы:

при разработке классификации КА необходимо руководствоваться наиболее общими принципами построения классификаций, способствующими правильному подбору оптимальных категорий и критериев для дальнейшей работы с созданной классификацией применительно к различным сферам обеспечения информационной безопасности;

при классификации КА предпочтение следует отдавать более общим, гибридным классификаторам. Классификации, основанные на учете ущерба, полученного информационными активами, и классификации, сосредоточенные на определенных типах атаки, не могут в достаточной мере отразить свойства и характеристики КА;

разрабатываемые классификации должны во всей полноте отвечать на следующие вопросы: «Кто совершает компьютерную атаку?», «Цель компьютерной атаки?», «Источник компьютерной атаки?», «Каков метод распространения атаки и каковы ее последствия для жертвы после инцидента?». Ответы на данные вопросы имеют большое значение для выбора стратегии защиты, предупреждения и прогнозирования атаки, ее своевременного обнаружения и противодействия проникновению в ИТКС.

Рассмотренные выше подходы не в полной мере отвечают всем этим требованиям.

Узел связи как основной элемент ИТКС и объект воздействия ка

На рис. 1 представлена обобщенная схема объекта ИТКС. Она распространена в критически важных отраслях, таких как сектор государственного и муниципального управления, банковская сфера, нефтяные компании, промышленный сектор и многие другие.

Открытый сегмент узла связи может состоять из следующих базовых элементов:

маршрутизатор;

коммутатор;

корпоративный сервер (на нем, как правило, работает корпоративный сайт компании);

локальная вычислительная сеть (ЛВС) и автоматизированные рабочие места (АРМ) открытого сегмента;

средства IP-телефонии АТС (по технологии VoIP), сопрягаемой с внешними ресурсами (городскими и междугородными телефонными сетями).

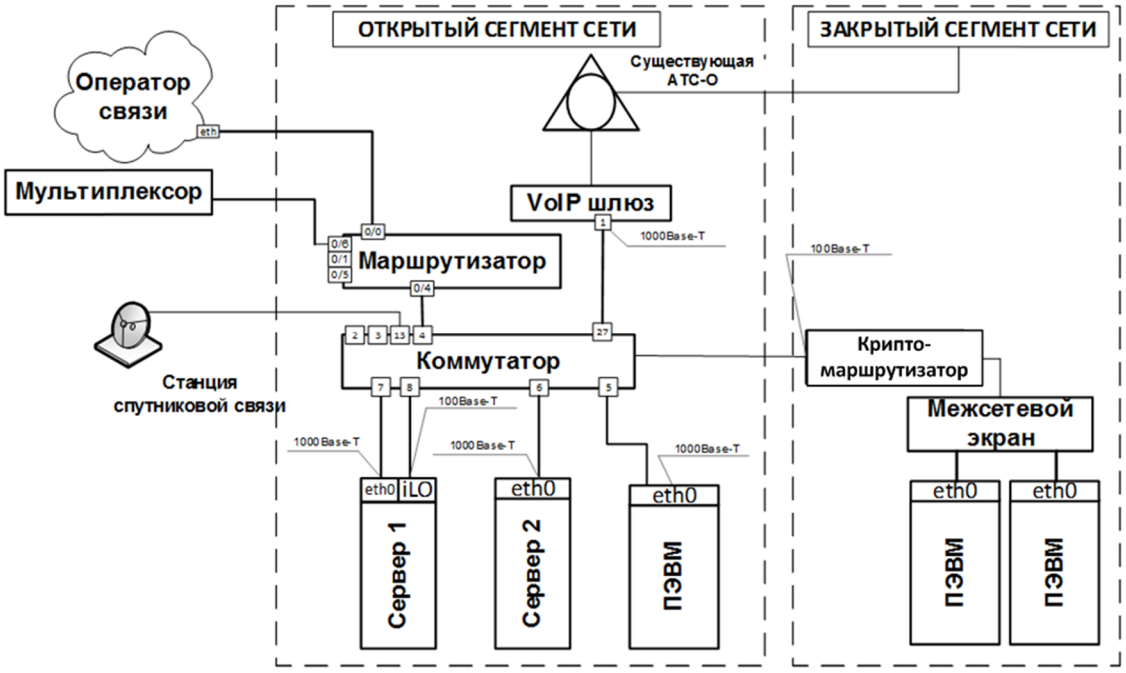

Рис. 1. Узел связи, как основной элемент ИТКС

В состав оборудования закрытого сегмента могут входить:

пограничный маршрутизатор либо межсетевой экран (если необходимо маршрутизировать трафик во внешнюю сеть, например в интернет);

криптомаршрутизатор;

коммутатор ЛВС;

ЛВС и АРМ закрытого сегмента;

средства IP-телефонии внутренней закрытой АТС, сопрягаемой с внешними ресурсами, но с обязательным условием криптозащиты и передачи трафика по туннелям виртуальной частной сети (VPN).

С точки зрения информационной безопасности криптомаршрутизатор и межсетевой экран или пограничный маршрутизатор обеспечивают криптографическую защиту информации на должном уровне. Однако это не даст стопроцентной защиты от компьютерных атак до тех пор, пока организация не научится минимизировать влияние человеческого фактора. Даже если перевести все узлы связи в режим тотальной автоматизации, исключив из процессов, связанных с обслуживанием ИТКС, человека, устранить риски, обусловленные доверительными отношениями, внутренними нарушителями, аппаратными или программными закладками и просто банальной неправильной настройкой сетевого оборудования, не представляется возможным.

Модель угроз маршрутизатору

Маршрутизатор является одним из самых уязвимых составляющих рассматриваемого объекта: это обусловлено главным образом тем, что он содержит таблицу маршрутизации. Это дает злоумышленнику большое преимущество в плане разведки корпоративной сети

изнутри. Захватив маршрутизатор, он может исследовать сеть на предмет выявления уязвимых соседей, чтобы, воспользовавшись их системами, проброситься в сеть глубже. Существует множество способов для этого. Все зависит от конкретной ситуации и типа маршрутизирующего устройства. В большинстве случаев можно подобрать логин и пароль специальными программами или воспользоваться средством Evil double.

При отсутствии потенциальных жертв, обменивавшихся данными с маршрутизатором, злоумышленник может наметить новые векторы атаки, направленные на распространение и скрытие следов взлома.

Поскольку маршрутизатор обменивается информацией с другими участниками сети, при его захвате не составит труда реализовать атаку «человек посередине» (MITM-атаку), перехватывать трафик или просто отключить любого участника от сети, выполнить проброс портов или вынудить администратора повторно ввести учетные данные с целью их перехвата и применения в другом узле сети.

Модель угроз коммутатору

Коммутатор является самым примитивным устройством объекта ИТКС. В большинстве случаев он не имеет таблицы маршрутизации и работает на канальном уровне. Коммутатор уязвим к ARP-атакам, направленным на «прослушивание» сетевого трафика, а также к DoS-атакам, нацеленным на канал связи. Его можно использовать для получения информации об элементах (пользователях) смежных сети.

Модель угроз серверу

В подавляющем большинстве случаев на сервере устанавливается операционная система Linux или Windows. В зависимости от операционной системы, а также от ее дистрибутива, конфигурация сервера, настройки сети и его предназначение могут существенно отличаться. Данная особенность сказывается на выборе варианта атаки. Первое, на что нужно обратить внимание, это перечень вариантов воздействий с помощью известных эксплойтов, доступных любому обывателю. Однако не следует забывать и о том, что сервер находится внутри сети. Поэтому для того, чтобы его атаковать, существуют три варианта со следующими результатами:

захвачен маршрутизатор, с помощью которого и производятся атаки;

на сервере запущен сайт, который доступен из сети интернет (самый распространенный вариант);

злоумышленник уже захватил сервер, но его права – пользовательские.

Модель угроз криптомаршрутизатору

Криптомаршрутизатор имеет собственную операционную систему, недоступную простому обывателю. Из-за того, что о нем никто ничего не знает, описать атаки и выявить уязвимости в его протоколах работы весьма сложно. Слабым местом криптомаршрутизатора может оказаться неправильная настройка протокола IPsec, а это шаг к дальнейшей расшифровке информации при наличии ключей шифрования от другого протокола, работающего в паре с IPsec. Кроме того, при отсутствии рекомендуемых настроек правил фильтрации или критических ошибках в настройках фильтров возможна реализация DoS-атак, направленных на нарушение работоспособности криптомаршрутизатора.

В перечень уязвимостей криптомаршрутизатора также входят доверительные отношения, внутренний нарушитель и аппаратные закладки.

Модель угроз межсетевому экрану

Основное предназначение систем межсетевого экранирования (firewall, FW) –защита внутренней пользовательской сети компании в составе сетей (интернет, интранет) стыка протоколов TCP/IP от случайного или целевого воздействия из внешней сети. Firewall включается в «разрыв» между внешней и внутренней (защищаемой) сетью.

Угрозы межсетевому экрану полностью аналогичны ранее рассматриваемым угрозам серверу, за тем исключением, что его операционная система, как правило, это Linux. Изделия FW имеют различные программно-аппаратные платформы и наборы интерфейсов в зависимости от конкретных целей заказчика и параметров конфигурации сопрягаемого оборудования (маршрутизаторов, коммутаторов, серверов и т.д.).

Сам процесс межсетевого экранирования представляет собой совокупность многофакторных проверок дейтаграмм по их аутентификации в соответствии с критериями безопасности. Однако, помимо этого, FW выполняет ряд фискально-контрольных функций: IP-фильтрация, NAT-обработка, туннелирование, proxy-сервер, регистрация событий. Таким образом, FW представляет собой комплексный набор инструментов предупреждения и защиты внутренней локальной вычислительной сети.

Модель угроз ПЭВМ

Достигнув оконечного узла сети – ПЭВМ, злоумышленник без труда сможет атаковать пользователя. Угрозы ПЭВМ полностью аналогичны ранее рассматриваемым для сервера.

В случае, если злоумышленнику не удастся проникнуть в закрытый сегмент сети и, всего лишь, «закрепившись» на АРМ открытого сегмента, он легко может захватить данные пользователей, среди которых, с большой долей вероятности, будут пароли администраторов сети. Не исключено, что эти пароли подойдут для элементов ИТКС закрытого сегмента

Заключение

Таким образом, в приведенных выше актуальных источниках информации предложены классификации КА, которые могут служить основой для исследования свойств атак и средств противодействия им. Однако известные классификации обобщают атаки в основном для сетей связи общего пользования (ССОП) типа интернета и, как правило, недостаточно информативны для сетей критически важного объекта инфраструктуры, в которых имеются особенности защищенного исполнения, хотя предъявляемые к ним требования жестче, чем к ССОП на несколько порядков [24].

В данном исследовании декомпозирована модель воздействий КА на ИТКС, разработанная на основе анализа соответствия между основными характеристиками элементов ИТКС, спецификой их применения и особенностями реализации КА. Модель представляет собой систематизированный перечень КА, воздействующих как на программное обеспечение элементов ИТКС, так и на субэлементы. Перечень угроз ИТКС, позволяет определить опасность, а также угрозу для каждого элемента сети.

Представленная классификация гармонично дополняет базовую модель информационной безопасности ФСТЭК и может эффективно использоваться при разработке частных моделей информационной безопасности для локальных сетей критически важного объекта инфраструктуры.

Анализ предложенной модели угроз показывает, что компьютерные атаки в большинстве своем универсальны и могут быть на любой элемент ИТКС, а их воздействия связаны с преднамеренным нарушением программного обеспечения и информации. Наибольшее количество воздействий направлены на серверы [25], ПЭВМ, а также на межсетевой экран.

Литература

1. *Карпов М.А., Лаута О.С., Коцыняк М.А., Крибель А.М.* Подход к управлению системой защиты информационно-телекоммуникационной сети специального назначения // Известия Тульского государственного университета. Технические науки. 2020. № 7. С. 216-226.

2. *Коцыняк М.А., Карпов М.А., Лаута О.С., Дементьев В.Е.,* Управление системой обеспечения безопасности информационно-телекоммуникационной сетью на основе алгоритмов функционирования искусственной нейронной сети // Известия Тульского государственного университета. Технические науки. 2020. № 4. С. 3-10.

3. *Paulauskas N., Garsva E.,* Computer System Attack Classification: ELECTRONICS AND ELECTRICAL ENGINEERING.

4. *Wei Jiang Zhi-hong Tian, Xiang. CUI* DMAT: A New Network and Computer Attack Classification: Journal of Engineering Science and Technology Review 6 (5).: 2018. Pp101-106.

5. *Chris Simmons, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, Qishi Wu,* AVOIDIT: A Cyber Attack Taxonomy.

6. *Mouna Jouinia, Latifa Ben Arfa Rabaia, Anis Ben Aissab*. Classification of security threats in information systems: 5th International Conference on Ambient Systems, Networks and Technologies (ANT-2019).

7. *RP van Heerden, B Irwin , ID Burke , L Leenen.* A computer network attack taxonomy and ontology.

8. Common Cyber Attacks Reducing The Impact// URL: https://www.ncsc.gov.uk/guidance/white-papers/common-cyber-attacks-reducing-impact (дата обращения: 10.09.22).

9. *Jason R. C. Nurse, Michael Goldsmith.* A taxonomy of cyber-harms Defining the impacts of cyber-attacks and understanding how they propagate Ioannis Agrafiotis, Journal of Cybersecurity.

10. *Daniel Pienta, Daniel Pienta, Allen C. Johnston.* A Taxonomy of Phishing Attack Types Spanning Economic, Temporal, Breadth, and Target Boundaries / Association for Information Systems AIS Electronic Library.

11. Cybersecurity Incident Taxonomy / NIS Cooperation Group // CG Publication 04/2018.

12. Towards a Cyber Conflict Taxonomy / Scott D. Applegate, Angelos Stavrou // 5th International Conference on Cyber Conflict 2019.

13. *Charles Harry, Nancy Gallagher.* Classifying Cyber Events A Proposed Taxonomy // CISSM Working Paper.: 2018.

14. *Aruna M., Gayathri K., Dr. Inbavalli M.* Network Security and Types of Attacks in Network Security / IOSR Journal of Engineering (IOSRJEN).

15. *Filippo Curti, Jeffrey Gerlach, Sophia Kazinnik, Michael Lee and Atanas Mihov.* Cyber Risk Definition and Classification for Financial Risk Management // Federal Reserve Bank of Richmond.

16. *Sagnik Basumallik.* A Taxonomy of Data Attacks in Power Systems / arXiv: .11011v1.:2020.

17. *Seungmin Kim, Gyunyoung Heo, Enrico Zio, Jinsoo Shin, Jae-gu Song.* Cyber attack taxonomy for digital environment in nuclear power plants / ELSEVIER Nuclear Engineering and Technology 50 (2020) 995-1001.

18. *Mohamed Amine Douad, Youcef Dahmani.* ARTT Taxonomy and Cyber-attack Framework / First International Conference on New Technologies of Information and Communication (NTIC).: 2019.

19. *Bonnie Zhu, Anthony Joseph, Shankar Sastry.* A Taxonomy of Cyber Attacks on SCADA Systems / 2019 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing.

20. *Md Mehedi Hassan Onik, Nasr Al-Zaben, Hung Phan Hoo, Chul-Soo Kim.* A Novel Approach for Network Attack Classification / Annals of Emerging Technologies in Computing (AETiC) Vol. 2, No. 2, 2018.

21. A *Tooska Dargahi, Ali Dehghantanha, Pooneh Nikkhah Bahrami, Mauro Conti, Giuseppe Bianchi, Loris Benedetto*. Cyber-Kill-Chain based taxonomy of crypto-ransomware features / Journal of Computer Virology and Hacking Techniques.: 2019. Pp.305

22. *Nikolaos Pitropakis, Emmanouil Panaousis, Thanassis Giannetsos, Eleftherios Anastasiadis, George Loukas.* A taxonomy and survey of attacks against machine learning / ELSEVIER Computers Science Review 100199.: 2019.

23. *Ian M. Chapman, Sylvain P. Leblanc, Andrew Partington.* Taxonomy of Cyber Attacks and Simulation of their Effects / Spring Simulation Multi-conference, SpringSim 11.: 2019.

24. *Карпов М.А., Коцыняк М.А., Лаута О.С., Муртазин И.Р., Коцыняк М.М.* Методика оценки защищенности структуры критически важного объекта информатизации от воздействий по ее несанкционированному вскрытию. Сборник: Состояние и перспективы развития современной науки по направлению «Информационная безопасность». сборник статей II Всероссийской научно-технической конференции. ФГАУ «Военный инновационный технополис «ЭРА». Анапа.: 2020. С. 37-41.

25. *Коцыняк М.А., Бударин Э.А., Карпов М.А., Муртазин И.Р., Иванов Д.А.* Воздействие нарушителя на беспроводные сети передачи данных по уровням эталонной модели взаимодействия открытых систем. Сборник: Состояние и перспективы развития современной науки по направлению «Информационная безопасность». сборник статей II Всероссийской научно-технической конференции. ФГАУ «Военный инновационный технополис «ЭРА». Анапа.: 2020. С. 139-146.

A MODEL OF THE IMPACT OF COMPUTER ATTACKS ON THE INFORMATION AND TELECOMMUNICATIONS NETWORK

OLEG S. LAUTA
PhD., Professor, St. Petersburg, Russia, laos-82@yandex.ru

DENIS A. IVANOV
PhD, Lecturer, Chelyabinsk, Russia, prosto_deniss@mail.ru

EDUARD V. AVEDYAN
PhD, Lecturer, Chelyabinsk, Russia, , avEddoV@mail.ru

ABSTRACT

Introduction: The paper presents a new approach to the classification of computer attacks on critical infrastructure objects, which takes into account from a comprehensive study of the object of impact to the implementation of the attack. **Problem statement:** Computer attacks on information and telecommunication networks, which are its key asset, are among the most noticeably increasing threats to the information security of a critical infrastructure facility. Modern targeted computer attacks represent a complex impact on the network, as a result of which the control of resources, hacking and infection of information and telecommunications networks. This is often preceded by a long and painstaking work in cyberspace: intelligence, the search for characteristic vulnerabilities and the seizure of information assets. The changing landscape of threats, the frequency of their occurrence, the complexity and the targeted nature of attacks - all this requires the evolution of the existing paradigm in the field of information security rules. **Methods:** method of conducting attacks; the method of forecasting and profiling computer attacks; the method of analyzing the logical topology of the network; the method of hidden Markov models. **Results**: the model is a systematized list of computer attacks affecting both the software of the elements of the information and telecommunications network, the specifics of their application and the features of the implementation of computer attacks, and the subelements. **Practical significance:** A list of threats to the information and telecommunications network, allows you to determine the danger, as well as the threat to each element of the network.

Keywords: critical infrastructure object; information system; classification; classifier; information and telecommunication network; computer network; information security; cyberspace; computer attack; network device.

REFERENCES

1. Karpov M.A., Lauta O.S., Kotsynyak M.A., Kribel A.M. Approach to the management of the information and telecommunication network protection system for special purposes // Proceedings of the Tula State Agricultural University. Technical sciences. 2020. No. 7. pp. 216-226.
2. Kotsynyak M.A., Karpov M.A., Lauta O.S., Dementiev V.E., Management of the information and telecommunication network security system based on artificial neural network functioning algorithms // Proceedings of Tula State University. Technical sciences. 2020. No. 4. pp. 3-10.
3. Paulauskas N., Garsva E., Computer System Attack Classification: ELECTRONICS AND ELEC-TRICAL ENGINEERING.
4. Wei Jiang Zhi-hong Tian, Xiang. CUI DMAT: A New Network and Computer Attack Classification: Journal of Engineering Science and Technology Review 6 (5).: 2018. Pp101-106.
5. Chris Simmons, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, Qishi Wu, AVOIDIT: A Cyber At-tack Taxonomy.
6. Mouna Jouinia, Latifa Ben Arfa Rabaia, Anis Ben Aissab. Classification of security threats in in-formation systems: 5th International Conference on Ambient Systems, Networks and Technologies (ANT-2019).
7. RP van Heerden, B Irwin , ID Burke , L Leenen. A computer network attack taxonomy and ontology.
8. Common Cyber Attacks Reducing The Impact// URL: https://www.ncsc.gov.uk/guidance/white-papers/common-cyber-attacks-reducing-impact (accessed: 10.09.22).
9. Jason R. C. Nurse, Michael Goldsmith. A taxonomy of cyber-harms Defining the impacts of cyber-attacks and understanding how they propagate Ioannis Agrafiotis, Journal of Cybersecurity.
10. Daniel Pienta, Daniel Pienta, Allen C. Johnston. A Taxonomy of Phishing Attack Types Spanning Economic, Temporal, Breadth, and Target Boundaries / Association for Information Systems AIS Electronic Library.
11. Cybersecurity Incident Taxonomy / NIS Cooperation Group // CG Publication 04/2018.
12. Towards a Cyber Conflict Taxonomy / Scott D. Applegate, Angelos Stavrou // 5th International Conference on Cyber Conflict 2019.
13. Charles Harry, Nancy Gallagher. Classifying Cyber Events A Proposed Taxonomy // CISSM Working Paper.: 2018.
14. Aruna M., Gayathri K., Dr. Inbavalli M. Network Security and Types of Attacks in Net-work Security / IOSR Journal of Engineering (IOSRJEN).
15. Filippo Curti, Jeffrey Gerlach, Sophia Kazinnik, Michael Lee and Atanas Mihov. Cyber Risk Definition and Classification for Financial Risk Management // Federal Reserve Bank of Richmond.
16. Sagnik Basumallik. A Taxonomy of Data Attacks in Power Systems / arXiv: .11011v1.:2020.
17. Seungmin Kim, Gyunyoung Heo, Enrico Zio, Jinsoo Shin, Jae-gu Song. Cyber attack taxonomy for digital environment in nuclear power plants / ELSEVIER Nuclear Engineering and Technology 50 (2020) 995-1001.
18. Mohamed Amine Douad, Youcef Dahmani. ARTT Taxonomy and Cyber-attack Frame-work / First International Conference on New Technologies of Information and Communication (NTIC).: 2019.
19. Bonnie Zhu, Anthony Joseph, Shankar Sastry. A Taxonomy of Cyber Attacks on SCADA Systems / 2019 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing.
20. Md Mehedi Hassan Onik, Nasr Al-Zaben, Hung Phan Hoo, Chul-Soo Kim. A Novel Approach for Network Attack Classification / Annals of Emerging Technologies in Computing (AETiC) Vol. 2, No. 2, 2018.
21. A Tooska Dargahi, Ali Dehghantanha, Pooneh Nikkhah Bahrami, Mauro Conti, Giuseppe Bianchi, Loris Benedetto. Cyber-Kill-Chain based taxonomy of crypto-ransomware features / Journal of Computer Virology and Hacking Techniques.: 2019. Pp.305
22. Nikolaos Pitropakis, Emmanouil Panaousis, Thanassis Giannetsos, Eleftherios Anastasiadis, George Loukas. A taxonomy and survey of attacks against machine learning / ELSEVIER Computers Science Review 100199.: 2019.
23. Ian M. Chapman, Sylvain P. Leblanc, Andrew Partington. Taxonomy of Cyber Attacks and Simulation of their Effects / Spring Simulation Multi-conference, SpringSim 11.: 2019.

24. Karpov M.A., Kotsynyak M.A., Lauta O.S., Murtazin I.R., Kotsynyak M.M. Methodology for assessing the security of the structure of a critically important informatization object from the effects of its unauthorized opening. Collection: The state and prospects of development of modern science in the direction of "Information security". collection of articles of the II All-Russian Scientific and Technical Conference. FSAU "Military innovative Technopolis "ERA". Anapa.: 2020. pp. 37-41.
25. Kotsynyak M.A., Budarin E.A., Karpov M.A., Murtazin I.R., Ivanov D.A. The impact of the intruder on wireless data transmission networks at the levels of the reference model of interaction of open systems. Collection: The state and prospects of development of modern science in the direction of "Information security". collection of articles of the II All-Russian Scientific and Technical Conference. FSAU "Military innovative Technopolis "ERA". Anapa.: 2020. pp. 139-146.