DOI: https://doi.org/10.15688/NBIT.jvolsu.2018.1.2

УДК 623.624
ББК 32.882

МЕТОДИКА ПРОГНОЗИРОВАНИЯ СТРУКТУРЫ ТАРГЕТИРОВАННОЙ КИБЕРНЕТИЧЕСКОЙ АТАКИ НА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННУЮ СЕТЬ

Владимир Витальевич Баранов

Кандидат военных наук, доцент, заведующий кафедрой информационной безопасности,
Южно-Российский государственный политехнический университет имени М.И. Платова
baranov.vv.2015@ yandex.ru
ул. Просвещения, 132, 346428 г. Новочеркасск, Российская Федерация

Михаил Антонович Коцыняк

Доктор военных наук, профессор,
Военная академия связи имени Маршала Советского Союза С.М. Буденного
kot-c@yandex.ru
Тихорецкий проспект, 6, 194064 г. Санкт-Петербург, Российская Федерация

Денис Александрович Иванов

Кандидат технических наук, преподаватель,
Военная академия связи имени Маршала Советского Союза С.М. Буденного
prosto_deniss@mail.ru
Тихорецкий проспект, 6, 194064 г. Санкт-Петербург, Российская Федерация

Аннотация. В статье рассмотрена проблема распространения таргетированных кибернетических атак в настоящее время, описан принцип их реализации. Также описана необходимость создания методики оценки воздействия ТКА противником на ИТКС и ее элементы, описана цель этой методики и ее структура. Перечислены этапы данной атаки, способы реализации и области ее проявления.

Ключевые слова: атака, таргетированная, ТКА, ИТКС, методика оценки воздействия, злоумышленник, матрица назначений.

Основной тенденцией последних лет называют смещение акцента с массовых атак на таргетированные, или целевые, которые заранее спланируют действия противника конкретной государственной или негосударственной структуры. Целевая атака всегда строится под объект воздействия, являясь продуманной операцией, а не простым техническим действием.

Таргетированная (целевая) кибернетическая атака (ТКА) на элемент информационно-телекоммуникационной сети (ИТКС) реализуется в виде проведения комплекса мероприятий по изучению информационной системы и программного обеспечения. На основе этого выявляются слабые места в структуре ИТКС. Разрабатывается техника скрытого внедрения и обхода стандартных средств защиты информации, осуществляется закрепление внутри инфраструктуры, распространяется и выполняется вредоносное действие.

В условиях воздействия ТКА затруднительно выбрать способы и средства защиты ИТКС, так как их ресурс ограничен. Одним из путей разрешения этого противоречия является дифференцированный подход к защите ИТКС, который заключается в выборе наиболее актуальных для сложившейся обстановки направлений защиты. Для обоснования направлений защиты ИТКС и ее элементов, ассиметричных возможностям ТКА, необходимо разработать методику оценки воздействия ТКА противником на ИТКС и ее элементы. В настоящее время отсутствуют методики, предназначенные для этого [3–5; 7; 10]. С целью устранения этого противоречия предлагается методика оценки воздействия ТКА на ИТКС.

Целью методики является прогнозирование распределения этапов ТКА с учетом места и роли элементов в ИТКС, определение очередности воздействия на элементы ИТКС, что позволит формировать исходные данные для принятия мер защиты элементов и ИТКС в целом.

Методика предназначена для обоснования принятия решений по защите элементов ИТКС от ТКА должностными лицами на этапах формирования, развертывания и функционирования ИТКС. Структура методики представлена на рисунке 1.

В настоящее время важной задачей обеспечения защищенности ИТКС является анализ воздействия таргетированной кибернетической атаки (ТКА). С учетом того, что данная атака является многофакторной, необходимо оценить стратегию воздействия ТКА на элементы ИТКС, что позволит реализовать дифференцированный подход к обеспечению информационной устойчивости ИТКС и ее элементов.

Результатами воздействия ТКА являются внедрение ложной информации; нарушение установленных регламентов сбора, обработки и передачи информации в автоматизированных системах управления; отказы, сбои в работе ИТКС; а также компрометация передаваемой (получаемой) информации.

Таргетированная кибернетическая атака на ИТКС реализуется в виде несанкционированного активного процесса в инфраструктуре сети, удаленно управляемого в реальном масштабе времени, с целью нарушения или снижения эффективности выполнения технологических циклов в ней.

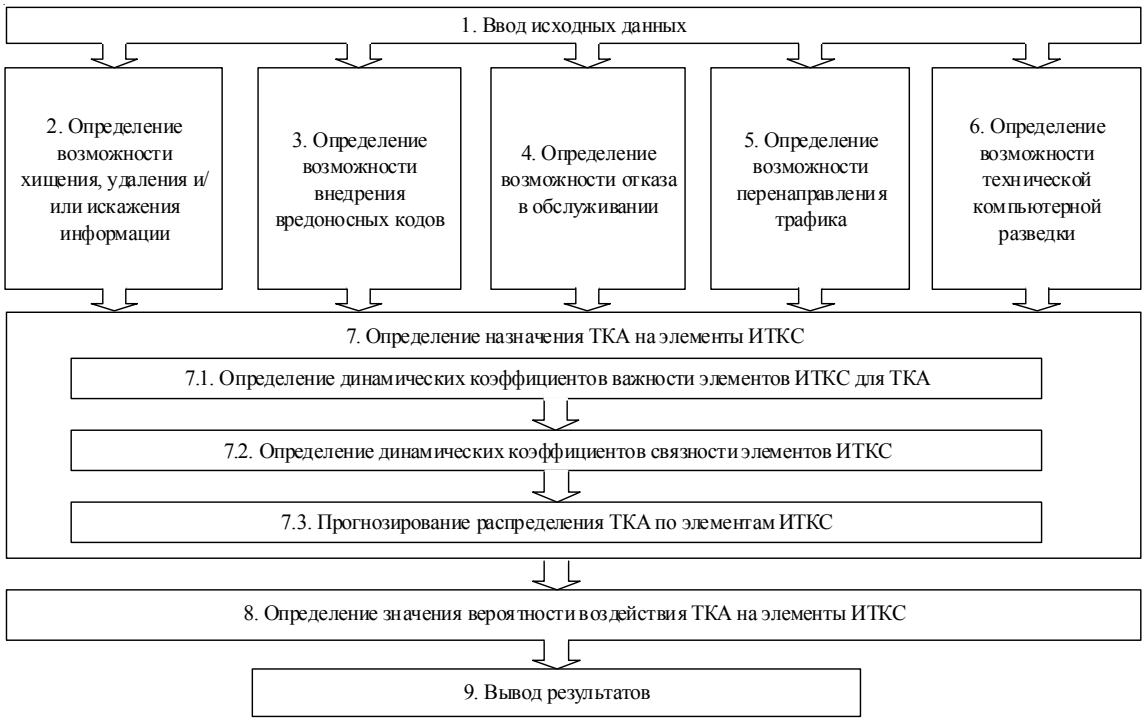

Рис. 1. Структура методики оценки комплексного информационного воздействия на ИТКС

Таблица 1

Анализ этапов ТКА

Этапы реализации ТКА	Способы реализации	Область проявления
I. Поиск (сетевое сканирование)	1.1 Анализ сетевого трафика	Канал связи
	1.2 Сканирование сети и ее уязвимостей	Коммутатор, Маршрутизатор, ПЭВМ, Серверы
	1.3 Сканирование протоколов передачи данных сети	
II. Создание стенда воздействий	2.1 Виртуальный	
	2.2 Аналитический	
	2.3 Имитационный	
III. Обход стандартных средств защиты	3.1. Обфускация модулей (вирусных сигнатур) с целью маскировки от антивирусов	Коммутатор, Маршрутизатор, ПЭВМ
	3.2 Выявление уязвимостей испытуемой системы	
	3.3 Инжектирование процесса (постэксплуатация)	
	3.4 Эксплуатация системы	
	3.5 Внедрение вирусных сигнатур в систему	
IV. Разработка набора инструментов	4.1 Средства создания инструментов воздействия	Коммутатор, Маршрутизатор, ПЭВМ, Серверы
	4.2 Тело вируса Payload	ПЭВМ
V. Закрепление внутри инфраструктуры	5.1 Инструменты эксплуатации	Коммутатор, Маршрутизатор, ПЭВМ, Серверы
VI. Мониторинг и выбор метода достижения цели	6.1 Хищение, удаление и/или искажение информации	ПЭВМ, Серверы
	6.2 Отказ в обслуживании	Коммутатор, Маршрутизатор, ПЭВМ, Серверы
	6.3 Перенаправление трафика	Маршрутизатор, ПЭВМ, Серверы

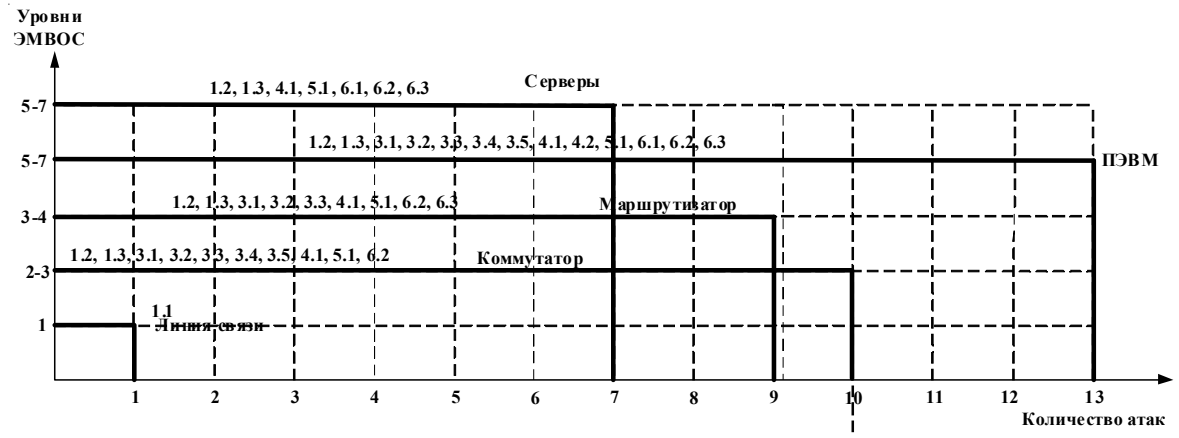

Рис. 2. Места проявления этапов ТКА в ИТКС

Анализ данных этапов ТКА (см. таблицу) позволяет сделать вывод о месте их проявления в ИТКС (рис. 2).

Анализ этапов ТКА и материалов по видам воздействий показывает, что воздействия на элементы ИТКС осуществляется как непосредственно на объекте, так и через транспортную сеть ИТКС. Общий характер проявления этапов ТКА на элементах ИТКС позволяет сделать вывод о том, что защита ИТКС от ТКА должна реализовываться в двух направлениях: защита транспортной сети, а также объектовая защита.

Для построения защиты ИТКС необходимо оценить ТКА, которые нанесут ущерб.

В настоящее время решение данной проблемы вызывает некоторое затруднение, связанное с недостаточной разработкой соответствующего методического аппарата. Поэтому для оценки опасности этапов ТКА для ИТКС предлагается использовать метод анализа иерархий.

Метод анализа иерархии (МАИ) применяется в тех случаях, когда перед лицом, принимающим решение, стоит проблема выбора решения из ряда альтернатив. Альтернативы характеризуются некоторыми весами, зная которые, не составляет труда выбрать наилучшую из них. Трудность состоит в том, что веса заранее неизвестны. Они могут быть получены применением метода, включающего в себя следующие этапы:

1. Постановка задачи и цель ее решения.

2. Построение иерархии задач.

3. Формирование матриц парных сравнений. Матрица строится для глобальной цели и для каждого из элементов промежуточных уровней.

4. Расчет собственных векторов и дополнительных величин по каждой из матриц парных сравнений.

5. Иерархический синтез оценок для получения искомых весов.

Определим показатель опасности КА для ИТКС с помощью МАИ.

Первым этапом применения МАИ является декомпозиция задачи выбора с использованием иерархии. В простейшем виде иерархия строится с вершины (цели) через промежуточные уровни-критерии (технико-экономические параметры) к самому нижнему уровню, который в общем случае является набором альтернатив.

После воспроизведения задачи в виде иерархии устанавливаются приоритеты критериев, и оценивается каждая из альтернатив. В МАИ элементы иерархии сравниваются попарно по их отношению к общей для них характеристике, что приводит к результату, который может быть представлен в виде обратно-симметричной матрицы $\|C_{ij}\|$. Элементом матрицы является оцениваемая важность элемента иерархии i относительно элемента иерархии j.

Каждый предмет можно оценивать по многим показателям. За степень опасности ТКА относительно вскрытия элементов ИТКС примем: степень воздействия на линию связи; степень воздействия на маршрутизатор; степень воздействия на коммутатор; степень воздействия на персональные электронно-вычислительные машины; степень воздействия на сервер электронной почты; степень воздействия на сервер базы данных; степень воздействия на сервер web.

Для формализации оценок экспертов в МАИ применяется шкала относительной важности.

Выбор градаций шкалы определен следующими условиями:

– шкала должна давать возможность улавливать разницу в ощущениях экспертов при проведении сравнений, различать как можно больше оттенков чувств, которые имеют эксперты;

– эксперт должен быть уверенным во всех градациях своих суждений одновременно.

Если при сравнении одного фактора i с другим j получено $c(i, j) = b$, то при сравнении второго фактора с первым получаем $c(i, j) = 1/b$.

Опыт показал, что при проведении парных сравнений i и j в основном ставятся следующие вопросы: «Какой из элементов иерархии важнее или имеет большее воздействие?»; «Какой из них более вероятен?»; «Какой из них предпочтительнее?».

Исходя из экспертных оценок строится матрица сравнений. Следующий шаг состоит в вычислении главного собственного вектора (СВ) матрицы, который после нормализации становится вектором приоритетов. Собственный вектор обеспечивает упорядочение приоритетов, а собственное значение является мерой согласованности суждений.

Следующим шагом является построение матриц сравнений степени опасности этапов ТКА по видам воздействия относительно цели, по способу реализации относительно видов воздействия, а также относительно элементов ИТКС с учетом их функционального распределения по уровням ЭМВОС. Этот шаг, по своей сути, аналогичен предыдущему, поэтому приведем только результаты решения названных матриц в виде нормализованных векторов-столбцов приоритетов степени опасности ТКА, выражающих весовые значения степени опасности ТКА (значения вероятностей).

Порядок построения матриц сравнений степени опасности этапов ТКА относительно каждого элемента ИТКС, по своей сути, аналогичен предыдущим.

Таким образом, используя метод анализа иерархий, представляется возможным определить степень воздействия на элементы ИТКС рассматриваемых этапов ТКА. Полученные результаты могут быть уточнены на этапе детального планирования при аналитической оценке защищенности ИТКС.

Результатом оценки воздействия на ИТКС будет матрица назначений ТКА противника на элементы ИТКС, а также очередность воздействия на них.

В основу методики положено определение степени опасности ТКА, для чего необходимо рассмотреть физические основы отдельных ТКА, особенности их воздействия, характер проявления на элементах ИТКС.

На основании результатов, полученных с использованием частных методик определения опасности этапов ТКА, разработаем методику оценки комплексного воздействия на ИТКС.

Учитывая идею распределения разноэффективных этапов ТКА по взаимозависимым с различной степенью важности элементам ИТКС, виды целевой функции и ограничений в условия решения задачи приемлемым методом решения является метод двух функций. Таким образом, разработана методика оценки комплексного информационного воздействия на основе распределения разнородного ресурса по взаимоувязанным элементам ИТКС, которая позволяет определить угрозы ИТКС и обосновать симметричные меры защиты. Данный метод позволяет оценить угрозы для элементов ИТКС по уровням эталонной модели и на каждом уровне формировать постановку задачи на синтез системы защиты ИТКС в условия воздействия ТКА.

СПИСОК ЛИТЕРАТУРЫ

1. Защита канала управления роботизированных систем / В. В. Баранов, М. А. Гудков, А. М. Крибель, О. С. Лаута, А. П. Нечепуренко // Актуальные проблемы обеспечения информационной безопасности : тр. Межвуз. науч.-практ. конф., г. Самара, 20–24 мая 2017 г. – Самара : Инсома-Пресс, 2017. – С. 32–37.

2. Кибербезопасность : Анализ нормативно-правовых документов Российской Федерации, регламентирующих политическую и военную деятельность в киберпространстве / М. А. Коцыняк, О. С. Лаута, В. О. Драчев, И. А. Клиншов // Материалы конференции ГНИИ «Нацразвитие». Ноябрь 2016 : сб. избранных статей. – СПб. : Нацразвитие, 2016. – С. 109–117.

3. Методика обоснования мер противодействия радиолокационной разведке высокоточного оружия / М. А. Коцыняк, В. В. Карганов, О. С. Лаута, А. П. Нечепуренко // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. – 2016. – № 9-10 (99-100). – С. 54–57.

4. Методика оценки защищенности информационно-телекоммуникационной сети в условиях информационного противодействия / М. А. Коцыняк, Д. А. Иванов, О. С. Лаута, А. П. Нечепуренко // Радиолокация, навигация, связь : сб. тр. XXIII Междунар. науч.-техн. конф. – Воронеж : Вэлборн, 2017. – С. 83–89.

5. Методика оценки устойчивости информационно-телекоммуникационной сети в условиях информационного воздействия / М. А. Коцыняк, О. С. Лаута, А. П. Нечепуренко, И. Г. Штеренберг // Труды учебных заведений связи. – 2016. – Т. 2, № 4. – С. 82–87.

6. Методика оценки устойчивости информационно-телекоммуникационной сети в условиях информационного воздействия / В. В. Баранов, М. А. Коцыняк, О. С. Лаута, В. М. Московченко // Вестник Волгоградского государственного университета. Серия 10, Инновационная деятельность. – 2017. – Т. 11, № 2. – С. 11–15. – DOI: https://doi.org/10.15688/jvolsu10.2017.2.2.

7. Модель таргетированной кибернетической атаки / М. А. Коцыняк, Д. А. Иванов, О. С. Лаута, А. П. Нечепуренко // Радиолокация, навигация, связь : сб. тр. XXIII Междунар. науч.-техн. конф. – Воронеж : Вэлборн, 2017. – С. 90–98.

8. Нормативно-правовые документы США, регламентирующие политическую и военную деятельность в киберпространстве / О. С. Лаута, В. В. Никитин, И. А. Клиншов, А. С. Лаута // Материалы конференции ГНИИ «Нацразвитие». Ноябрь 2016 : сб. избранных статей. – СПб. : Нацразвитие, 2016. – С. 118–125.

9. Применение метода топологического преобразования стохастических сетей для оценки эффективности средств защиты / В. В. Баранов, А. М. Крибель, О. С. Лаута, А. П. Нечепуренко //Актуальные проблемы обеспечения информационной безопасности : тр. Межвуз. науч.-практ. конф., г. Самара, 20–24 мая 2017 г. – Самара : Инсома-Пресс, 2017. – С. 47–52.

10. Саенко, И. Б. Применение метода преобразования стохастических сетей для моделирования

мобильных банковских атак / И. Б. Саенко, О. С. Лаута, И. В. Котенко // Известия высших учебных заведений. Приборостроение. – 2016. – Т. 59, № 11. – С. 928–933.

REFERENCES

1. Baranov V.V., Gudkov M.A., Kribel A.M., Lauta O.S., Nechepurenko A.P. Zashchita kanala upravleniya robotizirovannykh system [Protection of the Control Channel of Robotic Systems]. *Aktualnye problemy obespecheniya informatsionnoy bezopasnosti: trudy Mezhvuzovskoy nauchno-prakticheskoy konferentsii (Samara, 20-24 maya 2017)* [Relevant Problems of Information Security: Proceedings of the Interuniversity Scientific and Practical Conference (Samara, May 20-24, 2017)]. Samara, Insoma-Press, 2017, pp. 32-37.

2. Kotsynyak M.A., Lauta O.S., Drachev V.O., Klinshov I.A. Kiberbezopasnost: analiz normativno-pravovykh dokumentov Rossiyskoy Federatsii, reglamentiruyushchikh politicheskuyu i voennuyu deyatelnost v kiberprostranstve [Cybersecurity. Analysis of Regulatory Documents of the Russian Federation Regulating Political and Military Activities in Cyberspace]. Elzesser Yu.F., Pavlov L.A., eds. *Materialy konferentsii GNII "Natsrazvitie". Noyabr 2016. Sbornik izbrannykh statey* [Selected Proceedings of Conferences Held by GNII Natsraizvitie State National Research Institute. November 2016]. Saint Petersburg, Natsraizvitie Publ., 2016, pp. 109-117.

3. Kotsynyak M.A., Karganov V.V., Lauta O.S., Nechepurenko A.P. Metodika obosnovaniya mer protivodeystviya radiolokatsionnoy razvedke vysokotochnogo oruzhiya [The Method for Substantiation of Measures to Counteract Radar Reconnaissance of Precision Weapons]. *Voprosy oboronnoy tekhniki. Seriya 16: Tekhnicheskie sredstva protivodeystviya terrorizmu*, 2016, no. 9-10 (99-100), pp. 54-57.

4. Kotsynyak M.A., Ivanov D.A., Lauta O.S., Nechepurenko A.P. Metodika otsenki zashchishchennosti informatsionno-telekommunikatsionnoy seti v usloviyakh informatsionnogo protivodeystviya [Methodology for Assessing the Security of Information and Telecommunications Networks in the Context of Informational Countermeasures]. *Radiolokatsiya, navigatsiya, svyaz. Sbornik trudov XXIII Mezhdunarodnoy nauchno- tekhnicheskoy konferentsii* [Radar-location, Navigation, Communication. Collection of Proceedings of the 23rd International Scientific and Technical Conference]. Voronezh, Velborn Publ., 2017, pp. 83-89.

5. Kotsynyak M.A., Lauta O.S., Nechepurenko A.P., Shterenberg I.G. Metodika otsenki ustoychivosti informatsionno-telekommunikatsionnoy seti v usloviyakh informatsionnogo vozdeystviya [Methodology for Assessing the Stability of Information and Telecommunications Networks in the Conditions of Information Impact]. *Trudy uchebnykh zavedeniy svyazi*, 2016, vol. 2, no. 4, pp. 82-87.

6. Baranov V.V., Kotsynyak M.A., Lauta O.S., Moskovchenko V.M. Metodika otsenki ustoychivosti informatsionno-telekommunikatsionnoy seti v usloviyakh informatsionnogo vozdeystviya [Methodology for Assessing the Stability of Information and Telecommunications Networks in the Conditions of Information Impact]. *Vestnik Volgogradskogo gosudarstvennogo universiteta. Seriya 10, Innovatsionnaya deyatelnost* [Science Journal of Volgograd State University. Technology and Innovations], 2017, vol. 11, no. 2, pp. 11-15. DOI: https://doi.org/10.15688/jvolsu10.2017.2.2.

7. Kotsynyak M.A., Ivanov D.A., Lauta O.S., Nechepurenko A.P. Model targetirovannoy kiberneticheskoy ataki [The Model of the Targeted Cybernetic Attack]. *Radiolokatsiya, navigatsiya, svyaz. Sbornik trudov XXIII Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii* [Radar-location, Navigation, Communication. Collection of Proceedings of the 23rd International Scientific and Technical Conference]. Voronezh, Velborn Publ., 2017, pp. 90-98.

8. Lauta O.S., Nikitin V.V., Klinshov I.A., Lauta A.S. Normativno-pravovye dokumenty SShA, reglamentiruyushchie politicheskuyu i voennuyu deyatelnost v kiberprostranstve [Normative-Legal Documents of the USA Regulating Political and Military Activity in Cyberspace]. Elzesser Yu.F., Pavlov L.A., eds. *Materialy konferentsiy GNII "Natsrazvitie". Noyabr 2016. Sbornik izbrannykh statey* [Selected Proceedings of Conferences Held by GNII Natsraizvitie State National Research Institute. November 2016]. Saint Petersburg, Natsraizvitie Publ., 2016, pp. 118-125.

9. Baranov V.V., Kribel A.M., Lauta O.S., Nechepurenko A.P. Primenenie metoda topologicheskogo preobrazovaniya stokhasticheskikh setey dlya otsenki effektivnosti sredstv zashchity [Application of the Method for Topological Transformation of Stochastic Networks to Evaluate the Effectiveness of Protective Equipment]. *Aktualnye problemy obespecheniya informatsionnoy bezopasnosti: trudy Mezhvuzovskoy nauchno-prakticheskoy konferentsii* [Relevant Problems of Information Security: Proceedings of the Interuniversity Scientific and Practical Conference]. Samara, Insoma-Press, 2017, pp. 47-52.

10. Saenko I.B., Lauta O.S., Kotenko I.V. Primenenie metoda preobrazovaniya stokhasticheskikh setey dlya modelirovaniya mobilnykh bankovskikh atak [Application of the Method for Converting Stochastic Networks to Simulate Mobile Banking Attacks]. *Izvestiya vysshikh uchebnykh zavedeniy. Priborostroenie*, 2016, vol. 59, no. 11, pp. 928-933.

THE TECHNIQUE OF FORECASTING THE STRUCTURE OF TARGETED CYBER ATTACK ON INFORMATION TELECOMMUNICATION NETWORKS

Vladimir Vitalyevich Baranov

Candidate of Military Sciences, Associate Professor,
Head of Department of Information Security,
Platov South-Russian State Polytechnic University
baranov.vv.2015@yandex.ru
Prosveshcheniya St., 132, 346428 Novocherkassk, Russian Federation

Mikhail Antonovich Kotsynyak

Doctor of Military Sciences, Professor,
Military Academy of the Signal Corps named after S.M. Budenny
kot-c@yandex.ru
Prosp. Tikhoretskiy, 6, 194064 Saint Petersburg, Russian Federation

Denis Aleksandrovich Ivanov

Candidate of Sciences (Engineering), Lecturer,
Military Academy of the Signal Corps named after S.M. Budenny
prosto_deniss@mail.ru
Prosp. Tikhoretskiy, 6, 194064 Saint Petersburg, Russian Federation

Abstract. The main trend in recent years is the shift of emphasis from mass attacks to targeted (target) attacks, which are the actions of the enemy of a particular state or non-state structure in advance. The target attack is always built under the object of influence, being a thoughtful operation, not a simple technical action.

Target cyber attack on the element of information and telecommunication network is implemented in the form of a set of activities aimed at studying the information system and software. This allows for revealing weaknesses in the structure of the information and telecommunication network. The authors develop the technique of hidden introduction and bypass of standard means of information protection, fix the infrastructure, distribute the harmful action.

Under the impact of a targeted cyber attack, it is difficult to choose the methods and means of protecting the information and telecommunication network, as their resource is limited. One of the ways to resolve this contradiction is a differentiated approach to the protection of information and telecommunication network, which is to choose the most relevant for the current situation areas of protection.

The article deals with the problem of targeted attacks proliferation and describes the principle of their realization. The authors also substantiate the need of working out the methodology for estimating the impact of targeted cyber attacks by the enemy on information and telecommunications networks as well as their key elements. The special attention is paid to the purpose and structure of this methodology. The authors describe the stages of targeted cyber attack and its application areas.

Key words: attack, targeted attack, targeted cyber attack, information and telecommunications network, technique for estimating the impact, intruder, assignment matrix.