 DOI 10.25699/SSSB.2022.41.1.013

05.13.17

ОЦЕНКА ЗАЩИЩЕННОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ НА ОСНОВЕ ОБЩЕГО ГРАФА АТАК

В.С. Аверьянов[1], И.Н. Карцан[1,2,3]

[1]Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева, Красноярск, Россия

[2]Морской гидрофизический институт РАН, Севастополь, Россия

[3]Севастопольский государственный университет, Севастополь, Россия

Динамичное развитие IT – отрасли, повышение автоматизации и технологичности бизнес - процессов, рост числа организаций внедряющих облачную инфраструктуру, а также повсеместная цифровизация, создает благоприятную среду для масштабирования хакерских атак в сфере кибербезопасности. При этом векторами целевых атак являются: социальная инженерия, неквалифицированные пользователи цифровых сервисов, эксплуатация уязвимостей основных систем и сопутствующей инфраструктуры. Вопросы своевременного реагирования, локализации и выявления киберинцидентов являются насущными, требующими временных и финансовых затрат. Для минимизации рисков утраты критических активов компании, необходимо построение эффективных организационных и технических мер, непрерывная адаптация под ландшафт угроз и изменения в объекте защиты. Мероприятия по предотвращению вторжений в защищаемую систему напрямую зависят от точности определения уязвимых мест, внедрения новых средств мониторинга и противодействия. В настоящем исследовании рассмотрен метод оценки защищенности киберфизических систем на основе ориентированного графа атак. Авторами предложен алгоритм определения последовательностей вершин, нахождения максимального количества переходов и выявления возможных связей между ними. Описаны метрики безопасности и векторы атак, определены пять групп категорий опасностей для новых и существующих уязвимостей в соответствии с актуальной версией CVSS 3.1. Проведена оценка рисков потенциальных потерь информационных активов при возникновении фатальных угроз безопасности информации. Особое внимание уделено вопросам совершенствования систем мониторинга и обнаружения вторжений в защищаемые объекты информатизации.

Ключевые слова: граф вторжений, информационная безопасность, кибербезопасность, киберфизическая система, критический актив, оценка уязвимостей.

ВВЕДЕНИЕ

Киберпреступность как понятие сформировалось в начале 70-х годов прошлого века, у истоков исследовательского проекта ARPANET. В апреле 1973 года сотрудник компании BBN (Bolt Beranek and Newman) Боб Томас создал компьютерную программу Creeper, которая, «перемещаясь» по компьютерной сети Arpanet, оставляла цифровой след «I'm the creeper, catch me if you can» на ЭВМ (электронно-вычислительная машина). Позже, изобретатель электронной почты Рэй Томлинсон обнародовал программный код Reaper, который вычислял в компьютерной сети и удалял изобретение Боба Томаса. При этом программа представляла собой первое антивирусное ПО (программное обеспечение). Позже, модифицированный самовоспроизводившийся код сделал её сетевой уязвимостью – компьютерным червём. Так было положено начало поиску и эксплуатации уязвимостей в открытых компьютерных сетях связи общего назначения. С тех пор мало что изменилось, а наличие «брешей» в киберфизических системах является актуальной и важной проблемой для граждан, бизнеса и государственных структур, имеющих доступ к глобальным информационным системам. При этом каждое новое подключаемое оборудование представляет собой угрозу безопасности для окружающей информационной инфраструктуры, нуждаясь в превентивных мерах защиты.

В современных реалиях Интернет стал доступен каждому практически с рождения и сложно представить сферу деятельности человека, где его «цифровой след» отсутствует. Ежедневно на мировых IT-рынках появляются десятки, порой и сотни новых ПО, инновационных технических устройств, киберпространств, полигонов и площадок для дискуссий в сфере IT-технологий. Несомненно, столь резкий скачок в развитии кибернетических систем упрощает жизнь, позволяя человеку шагать в ногу со временем. Но есть и обратная сторона – перед злоумышленниками или, иначе говоря, киберпреступниками открылись новые безграничные возможности, направленные на нарушение основных свойств ИБ [1] (информационной безопасности).

К числу масштабных кибератак в 2021 году следует отнести: атака REvil на Kaseya, где злоумышленники использовали уязвимость 0-day и атаковали клиентов компании, атака группировки Hive на Memorial Health Systemc хищением более 1,5 ТБ персональных данных и многие другие[12]. При этом выстроенный наспех цифровой мир, в

фундамент которого заложены не базовые принципы ИБ и киберустойчивости, а экономические показатели и скорость вывода продуктов на рынок является достаточно хрупким и уязвимым. Самым слабым звеном остается эксплуатация уязвимостей нулевого дня, а эксплойты позволяют хакерам компроментировать сети связи, создав при этом киберинциденты для крупных корпоративных информационных систем и причиняя непоправимый экономический ущерб деятельности и деловой репутации компаний.

Все более значимым становится влияние регуляторов в области ИТ и ИБ. Вовлеченность в вопросы информационной безопасности стратегически важных государственных объектов и игроков крупного бизнеса, обязывают компании и государственные структуры внедрять средства защиты от внешних и внутренних угроз, без исключения. При этом существует ряд предпосылок на усиление регулирования в новом 2022 году: указ Президента РФ №213 от 12.04.2021 «об основах государственной политики РФ в области международной информационной безопасности», выпуск новых ГОСТов по ИБ, и многое другое. Соответствовать стандартам – трудоемкая, в большинстве случаев экономически затратная задача, но незащищенные информационные активы обходятся в десятки раз дороже, в случае хакерской атаки и утечке критически важных данных.

Для решения актуальных задач киберзащиты, соответствия перечню требований регулятора, компании внедряют различные механизмы и технические решения для поиска уязвимостей [2]и устранения источников потенциальных угроз. Компоненты информационной защиты современных IT-инфраструктур представлены на рис. 1

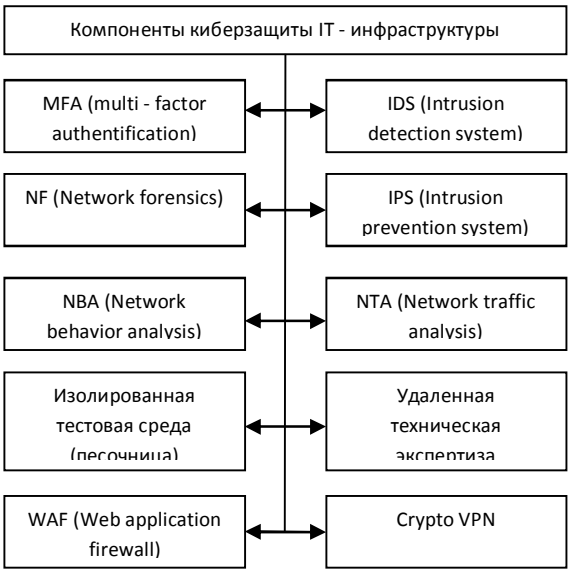

Рис. 1. Компоненты киберзащиты IT-инфраструктуры

Как видно из рис. 1 вопросы кибербезопасности компаний являются задачей, состоящей из множества элементов. Взаимосвязь элементов позволяет создавать IT-подразделениям единую гибридную систему своевременного обнаружения и предупреждения киберугроз, а также внедрять механизмы контроля доступа с «нулевым доверием». Построение результативной защиты позволит обрабатывать и анализировать множество событий из различных источников, а также предоставит специалистам по ИБ необходимый инструментарий для реагирования на киберинцинденты и позволит предотвращать недопустимые катастрофические последствия для бизнеса.

ОСНОВНАЯ ЧАСТЬ

К одной из методик выявления и локализации возможных несанкционированных действий злоумышленника в киберпространстве относится граф [4] вторжений или атак. В проведенном исследовании представлялось интересным рассмотреть ориентированный граф, где каждая из преднамеренных целевых атак реализуется на уязвимостях «нулевого дня» киферфизических систем. Метод оценки защищенности включает в себя алгоритм по формированию последовательностей вершин графа, нахождении максимального количества переходов и выявлении возможных связей между ними. При этом множество вершин представляют собой действия дестабилизирующего характера, иначе говоря - УБИ (угроза безопасности информации) [6]. Дуги соединяющие между собой вершины графа – уязвимости системы и новые эксплойты, с помощью которых происходит нарушение «спокойствия» киберсистемы, и возможный успех реализации одной или нескольких УБИ.

К числу объектов при построении ориентированного графа атак следует отнести: «маршрут» атаки, «уязвимость» системы [3] и «эффективность» противодействия. Маршрут целевой атаки представляет собой совокупность связей вершин графа, где первая из вершин соответствует начальному положению нарушителя, последняя не имеет продолжения и является конечным состоянием системы. Под уязвимостью киберсистемы следует понимать всевозможные маршруты атак, имеющих начало и конечную вершину. При этом совокупность вершин графа позволяет ввести понятие УБИ, соотнести их с уязвимостями и произвести классификацию по степени опасности для информационного ресурса. Классификация УБИ по механизмам воздействия представлена на рис. 2

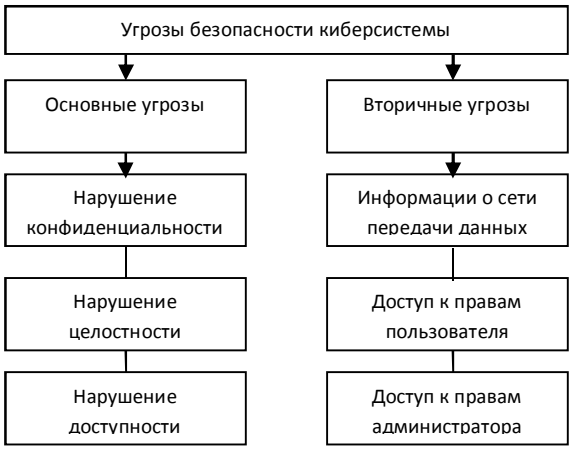

Рис. 2. Классификация угроз безопасности на основе общего графа

При этом сценарий развития атакующих воздействий киберпреступника на информационную систему можно представить как:

- начальное состояние нарушителя в киберфизической системе Y_0;
- УБИ, согласно банка данных угроз безопасности информации Y_{in}.
- существующие уязвимости конкретной УБИ $Y_1 \ldots . Y_i$;

Основой для эффективного построения графа атак, его анализа и внедрения соответствующих механизмов защиты служат данные открытых стандартов CVSS v3.1 [7], CPE (Common Platform Enumiration) [7], CCE (Common Configuration Enumiration) [9] и база NVD (National Vulnerabillity Database) [10]. Стандарт CVSS v3.1 описывает маршруты между вершинами графа и необходим для оценки показателей защищенности киберсистемы. CPE и CCE позволяют подобрать необходимый набор программно-аппаратного обеспечения, определить возможные уязвимости его конфигураций. NVD – база данных уязвимостей способствует автоматизации процессов анализа защищенности киберфизических систем.

Рассмотрим метод оценки защищенности киберфизических систем на основе построения ориентированного графа атак, формирования переходов и выявлении связей между его вершинами. С целью определения вершин и построения дуг графа введем компонент M_s, который представляет собой маршрут несанкционированных воздействий на систему Y. При этом общее количество связей в графе атак имеет вид: $M_s = M_{y0} + \cdots + M_{ys}$.

Алгоритм включает в себя определение УБИ, поиск уязвимостей киберфизической системы Y и состоит из следующих этапов:

1. Этап формирования. Данный этап предполагает выявление возможных УБИ киберсистемы Y_{in}, начального положения нарушителя в системе Y, а также формирование вершин графа и поиск множества уязвимостей $Y_1 \ldots . Y_i$. по принадлежности к Y_{in}.

2. Этап инициирования. На данном этапе происходит присвоение метрик Exploitability или Impact вершинам Y_i, согласно CVSS v 3.1 для каждой из сформированных последовательностей.

3. Этап определения дуг графа. На данном этапе происходит определение всевозможных переходов и построение маршрутов M_s атакующих воздействий киберпреступника в системе Y.

4. Этап анализа рисков ИБ. На данном этапе происходит конечное формирование уязвимостей $Y_1 \ldots . Y_i$., распределение их в графе атак по классу опасности, исходя из ранее определенных метрик присвоенных вершинам графа Y_i,

5. Этап оценки защищенности. На данном этапе происходит оценка защищенности исследуемой киберфизической системы Y, исходя из общего количества сформированных маршрутов атаки $M_s = M_{y0} + \cdots + M_{ys}$, степени опасности уязвимостей и критичности информационного ресурса, на который направлено дестабилизирующее воздействие.

В том числе, процесс мониторинга киберфизических систем, оценка уровня защищенности эксплуатируемой информационной системы происходит на основе сформированного графа атак и ряда различных метрик безопасности. Используемые метрики при формировании ориентированного графа экспоненциально влияют на процессы оценки защищенности. Чем больше метрик используется при моделировании графа, тем точнее и эффективнее будет результат. CVSS версии 3.1 включает в себя две группы метрик: Exploitability и Impact. Первая из них характеризуют уязвимый компонент киберсистемы: вектор атаки, сложность атаки, необходимые привилегии доступа, взаимодействие с пользователем системы [6]. Группа Impact необходима для отображения последствий вторжений атакующего, позволяет оценить влияние на основные критерии ИБ: целостность, доступность, конфиденциальность. При этом переход к новой версии CVSS v3.1 в отличии от версии 2.0 позволяет произвести модификацию вычисления показателей защищенности системы.

Алгоритм формирования графа атак, определение вершин в виде УБИ, возможных смежных переходов и выявление основных и второстепенных связей представлен на рис.3

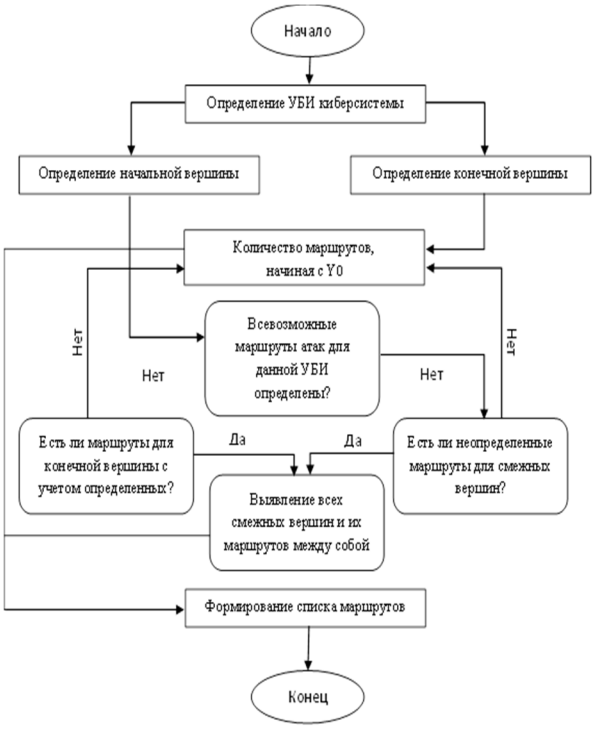

Рис. 3. Алгоритм поиска маршрутов атак на киберсистему

Согласно рисунку 3 структура графа атак имеет следующий вид: начальное положение киберпреступника в системе → угроза безопасности → уязвимость системы → эффективность действий злоумышленника → анализ оценки защищенности системы.

Результатом работы алгоритма является определение возможных сценариев и маршрутов атак на защищаемую информационную систему, а также набор данных об уязвимостях представленный в таблице 1.

Табл. 1. Маршрут атаки и набор данных об уязвимостях системы

№ п/п	Маршрут атаки	Уровень опасности	Индекс УБИ	Индекс метрик
Уязвимости первого порядка				
1	$M_{y0} \rightarrow \rightarrow M_{y1} \ldots \rightarrow M_{ys}$	низкий	Y_{in}	$EX(Y_{in})$, $AC(Y_{in})$,
2	$M_{y0} \rightarrow \rightarrow M_{y1} \ldots \rightarrow M_{ys}$	средний	Y_{in}	$EX(Y_{in})$, $AC(Y_{in})$,
Уязвимости второго порядка				
3	$M_{y0} \rightarrow \rightarrow M_{y2} \ldots \rightarrow M_{ys}$	средний	Y_{in}	$EX(Y_{in})$, $AC(Y_{in})$,
4	$M_{y0} \rightarrow \rightarrow M_{y2} \ldots \rightarrow M_{ys}$	высокий	Y_{in}	$EX(Y_{in})$, $AC(Y_{in})$,
5	$M_{y0} \rightarrow \rightarrow M_{y2} \ldots \rightarrow M_{ys}$	критический	Y_{in}	$EX(Y_{in})$, $AC(Y_{in})$,
Уязвимости третьего порядка				
6	$M_{y0} \rightarrow \rightarrow M_{y3} \ldots \rightarrow M_{ys}$	высокий	Y_{in}	$EX(Y_{in})$, $AC(Y_{in})$,
7	$M_{y0} \rightarrow \rightarrow M_{y3} \ldots \rightarrow M_{ys}$	критический	Y_{in}	$EX(Y_{in})$, $AC(Y_{in})$,
8	$M_{y0} \rightarrow \rightarrow M_{y3} \ldots \rightarrow M_{ys}$	фатальный	Y_{in}	$EX(Y_{in})$, $AC(Y_{in})$,

Уязвимости, обуславливающие наличие УБИ, а также их классификация по уровню опасности для защищаемого информационного актива позволяют сформировать сценарий целевой атаки в виде ориентированного графа, представленного на рис.4.

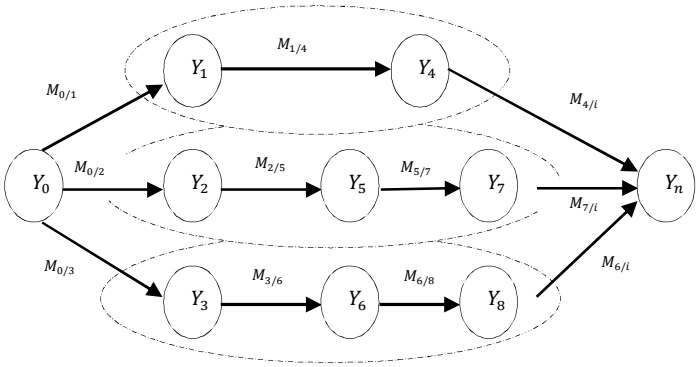

Рис. 4. Сценарий вторжения в защищаемую информационную инфраструктуру

Далее рассмотрим некоторые показатели защищенности киберфизической системы:

– *AccessComplexity* – сложность атакующего воздействия *a* и предоставления доступа к киберсистеме. Переход к версии 3.1 привел к изменению формулы данного показателя, в том числе авторами предложен новый показатель *«Fatal»*:

$$AccessComplexity = AttackComplexity(a),$$

$$AttackComplexity(a) = \begin{cases} None, \exists k \epsilon [1, M_s]: AttackComplexity(S_k) = None, \\ Low, \exists k \epsilon [1, M_s]: AttackComplexity(S_k) = Low, \\ Medium, \exists k \epsilon [1, M_s]: AttackComplexity(S_k) = Medium, \\ High, \exists k \epsilon [1, M_s]: AttackComplexity(S_k) = High, \\ High, \exists k \epsilon [1, M_s]: AttackComplexity(S_k) = Fatal, \end{cases}$$

где *AttackComplexity (a)* – сложность атаки для уязвимостей по маршруту M_s создающих угрозу безопасности $a = \{S_k\}_{k=1}^{M_s}$, при атакующем количестве S_k воздействии a на киберфизическую систему.

Тогда оценка возможного ущерба находится в прямой зависимости от: атакующего воздействия a, степени реализации угрозы безопасности $a = \{S_k\}_{k=1}^{M_s}$, и критичности информационного актива. При использовании CVSS версии v3.1 показатель определяется следующим образом:

$$AttackImpact = Realization(a) \propto Criticality(In, Av, Pr),$$

$$AttackImpact(a) = \begin{cases} None, AttackComplexity(a) = None, \\ Low, AttackComplexity(a) = Low, \\ Medium, AttackComplexity(a) = Medium, \\ High, AttackComplexity(a) = High, \\ Fatal, AttackComplexity(a) = Fatal. \end{cases}$$

Исходя из последнего релиза системы CVSS v3.1 показатели возможного ущерба определены как: целостность (In), доступность (Av), конфиденциальность (Pr). Всевозможные сочетания показателей от атакующего воздействия *a:* In, Av, Pr, InAv, InPr, AvPr, InAvPr и без ущерба как none. В связи с этим перечень угроз и защитных мер определяются индивидуально для каждой защищаемой киберсистемы.

ЗАКЛЮЧЕНИЕ

В рассматриваемой статье проанализирована методика оценки уровня защищенности киберфизических систем на основе метрик безопасности и алгоритма построения ориентированного графа целевых атак. За основу принята новая версия системы оценки уязвимостей CVSS v3.1 с введением нового показателя опасности «фатальный». Предложенный авторами алгоритм позволяет: во-первых, определять всевозможные маршруты несанкционированных многошаговых деструктивных воздействий; во-вторых, выявлять существующие угрозы кибербезопасности защищаемой системы и в-третьих, проводить оценку потенциального экономического ущерба от реализованных атак. На основе проведенного анализа сделан вывод, о том, что применение модифицированной версии стандарта CVSS позволяет более объективно оценить уровень защищенности информационной системы, а также возможный ущерб критически важным активам компании. Результаты работы послужат созданию алгоритма выработки верных и обоснованных решений по устранению уязвимостей. К практической части следует отнести повышение уровня защищенности конкретной анализируемой киферфизической системы. Кроме того, в последующих работах авторов представляется интересным реализовать программную часть генерации графов атак с автоматизированным выбором защитных механизмов на основе NVD и апробацией результатов на конкретной семантически стойкой криптосистеме.

Работа выполнена в рамках государственного задания по теме № 0555-2021-0005.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Абрамов М.В., Тулупьев А.Л., Сулейманов А.А. Задачи анализа защищенности пользователей от социоинженерных атак: построение социального графа по сведениям из социальных сетей. Научно-технический вестник информационных технологий, механики и оптики, 2018 г. т.18 №2, 313-321 с.

2. Averyanov V.S. Vulnerability of modern IPS/IDS systems. Молодежь. Общество. Современная наука, техника и инновации. – 2020. - №19. – P.273-275.

3. Аверьянов В.С, Карцан И.Н. Уязвимости современных IPS/IDS систем // Актуальные проблемы авиации и космонавтики: Сборник материалов VI Международной научно - практической конференции посвященной дню космонавтики / Под ред. Ю.Ю. Логинова. – Красноярск: СибГУ им. М.Ф. Решетнева, 2020, 194-197 с.

4. Дойникова Е.В., Котенко И.В. Методики и программный компонент оценки рисков на основе графов атак для систем управления информацией и событиями безопасности // информационно – управляющие системы. 2016. №5. С.54-65.

5. Barnum S. Common Attack Pattern Enumiration and Clasification (CAPEC).- Schema Description, 2008. – 26p.

6. Федеральная служба по техническому и экспортному контролю // URL: https://bdu.fstec.ru (дата обращения 19.11.2021).

7. Inglos K., Lippmann R., Piwowarski K. Practical Attack Graph Generation for Network Defense // Proc. of 22nd Annual Conf. on the Computer Security Applications, Miami Beach, FL. IEEE, 2006. P. 121-130.

8. Common Vulnerability Scoring System (CVSS v3.1). NVD website. URL: https://nvd.nist.gov/vuln – metrisc/cvss/v3.cfm (дата обращения 19.11.2021).

9. Common Platform Enumiration (CPE). NVD website. URL: https://nvd.nist.gov/cpe.cfm (дата обращения 20.11.2021).

10. Common Configuration Enumiration (CCE). NVD website. URL: https://nvd.nist.gov/cce/index.cfm (дата обращения 20.11.2021).

11. NVD website. URL: https://nvd.nist.gov (дата обращения 21.11.2021).

12. Самые громкие взломы и утечки 2021 года. //URL: https://habr.com/ru/company/pt/blog/598845 (дата обращения 25.12.2021).

Аверьянов Виталий Сергеевич – аспирант ФГБОУ ВО «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева», e-mail: averyanov124@mail.ru.

Карцан Игорь Николаевич – доктор технических наук, доцент, профессор Севастопольского государственного университета, старший научный работник ФГБУН ФИЦ «Морской гидрофизический институт РАН»,e-mail: kartsan2003@mail.ru.

ASSESSMENT OF THE SECURITY OF CYBER-PHYSICAL SYSTEMS BASED ON A GENERAL GRAPH

V.S. Averyanov[1], I.N. Kartsan[1,2,3]

[1]Reshetnev Siberian State University of Science and Technology, Krasnoyarsk, Russia
[2]Marine Hydro-physical Institute, Russian Academy of Sciences, Sevastopol, Russia
[3]Sevastopol State University, Sevastopol, Russia

The dynamic development of IT - the industry, increasing the automation and technicality of business processes, the growth of the number of enterprise companies implementing cloud infrastructure, as well as widespread digitalization, creates a favorable environment for scaling hacker attacks in the field of cybersecurity. At the same time, the vectors of targeted attacks are: social engineering, unskilled users of digital services, the operation of vulnerabilities of basic systems and related infrastructure. Issues of timely response, localization and detection of cyber-incidents were urgent, requiring time and financial costs. To minimize the risk of loss of critical assets of the company, it is necessary to build effective organizational and technical measures, continuous adaptation to the threat landscape and changes in the protection object. Measures to prevent intrusions into the protected system directly depend on the accuracy of identifying vulnerabilities, the introduction of new monitoring and countermeasures. The present study discusses a method for assessing the security of cyberphysical systems based on an oriented attack graph. The authors propose an algorithm for determining sequences of vertices, finding the maximum number of transitions and identifying possible connections between them. Security metrics and attack vectors are described, five groups of hazard categories for new and existing vulnerabilities are defined in accordance with the current version of CVSS 3.1. The risk of potential loss of information assets in case of fatal threats to information security was assessed. Special attention is paid to improvement of systems of monitoring and detection of intrusions into protected objects of informatization.

Index terms: intrusion graph, information security, cybersecurity, cybersystem, critical asset, vulnerability assessment.

REFERENCES

1. Abramov M.V., Tulupyev A.L., Sulejmanov A.A. Problem of analysis of user protection from social engineering attacks: construction of the social graph on information from social network websites. Nauchno-tekhnicheskij vestnik informatsionnyh tekhnologij, mekhaniki i optiki, 2018. vol. 18, no 2, p. 313-321.
2. Averyanov V.S. Vulnerability of modern IPS/IDS systems. Young people. Overview. Modern science, technology and innovation. – 2020. - №19. - P.273-275.
3. Averyanov V.C, Kartsan I.N. Vulnerabilities of modern IPS/IDS systems//Current problems of aviation and cosmonautics: Collection of materials of the VI International Scientific and Practical Conference dedicated to the day of cosmonautics/Ed. Yu.Yu. Loginova. - Krasnoyarsk: SibSU named after M.F. Reshetneva, 2020, P. 194-197.
4. Doinikova E.V., Kotenko I.V. Techniques and software component of risk assessment based on attack graphs for information and security event management systems//information and control systems. 2016. №5. S.54-65.
5. Barnum S. Common Attack Pattern Enumiration and Clasification (CAPEC).- Schema Description, 2008. – 26p.
6. Federal Service for technical and export control. website., accessed November 19, 2021, https://bdu.fstec.ru
7. Inglos K., Lippmann R., Piwowarski K. Practical Attack Graph Generation for Network Defense // Proc. of 22nd Annual Conf. on the Computer Security Applications, Miami Beach, FL. IEEE, 2006. P. 121-130.
8. Common Vulnerability Scoring System (CVSS v3.1). NVD website., accessed November 19, 2021, https://nvd.nist.gov/vuln – metrisc/cvss/v3.cfm.
9. Common Platform Enumiration (CPE). NVD website., accessed November 20, 2021, https://nvd.nist.gov/cpe.cfm.
10. Common Configuration Enumiration (CCE). NVD website. , accessed November 20, 2021, https://nvd.nist.gov/cce/index.cfm.
11. NVD website. , accessed November 21, 2021, https://nvd.nist.gov.
12. The loudest hacks and leaks of 2021. website., accessed December 12, 2021, https://habr.com/ru/company/pt/blog/598845 (дата обращения 25.12.2021).

Kartsan Igor Nikolaevich – Dr. Sc., Senior Researcher, Marine Hydrophysical Institute, Russian Academy of Science , Reshetnev Siberian State University of Science and Technology. Professor, Sevastopol State University, e-mail: kartsan2003@mail.ru.

Averyanov Vitaliy Sergeevich – graduate student of Reshetnev Siberian State University of Science and Technology, e-mail: averyanov124@mail.ru.