УДК 004.056

Шихвердиева А.Ш., Максимова Е.А.

ОЦЕНКА ДЕСТРУКТИВНОГО ВОЗДЕЙСТВИЯ НА СУБЪЕКТЫ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Аннотация. В связи с высоким риском информационной безопасности сфер, к котором отнесены субъекты критической информационной инфраструктуры (СКИИ), появляется необходимость в разработке комплексной оценке деструктивного воздействия на них. Предлагается подход оценки деструктивного воздействия на СКИИ, основанный на жизненном цикле, который характеризует субъект не зависимо от сферы его функционирования. Предлагается шкала оценки уровня критичности деструктивного воздействия на СКИИ.

Ключевые слова: критическая информационная инфраструктура, субъект, жизненный цикл, деструкт, деструктивное воздействие, сети Петри, уровень критичности, модель.

Abstract. Due to the high risk of information security in the areas to which the subjects of critical information infrastructure (SCII) are assigned, it becomes necessary to develop a comprehensive assessment of the destructive impact on them. The approach of assessing the destructive impact on SCII based on the life cycle that characterizes the subject regardless of the scope of its functioning is proposed. A scale for assessing the criticality level of destructive impact on SCII is proposed.

Keyword: critical information infrastructure, subject, life cycle, destruction, destructive impact, Petri nets, criticality level, model.

Введение

В Российской Федерации о критической информационной инфраструктуре (КИИ) заговорили в 2017 году, после утверждения Федерального закона от 26.07.2017 N 187-ФЗ [1]. В сравнении с мировым опытом, Россия несколько отстала в данном вопросе [2]. Американская президентская директива PDD-63 в мае 1998 года учредила национальную программу «Защита критической инфраструктуры» [3]. В то время как Россия занялась данным вопросом в теории, большинство стран Европы уже активно занимаются защитой КИИ и имеют в данном вопросе значительный опыт [4].

К наиболее опасным и подверженным угрозам отраслей входят энергетика, нефтегаз, транспорт и водоснабжение [5]. Также следует обратить внимание, что среди юридических лиц наиболее часто злоумышленники атакуют государственные организации, медицинские учреждения, промышленные компании, банки и другие организации финансовой сфере [6]. Большая часть отраслей, популярных для атак, относятся к отраслям КИИ.

Опираясь на определение деструктивного воздействия [7], под деструктом КИИ будем понимать фактор, угрозу, ошибку, предмет или способ реализации того, что ведет к неблагоприятным и разрушительным последствиям для СКИИ.

Деструктивное воздействие на СКИИ можно рассматривать на глобальном и локальном уровнях. Глобальный уровень подразумевает косвенное деструктивное воздействие на СКИИ. Реализация успешной атаки на СКИИ влечет за собой косвенное воздействие на другие СКИИ, которые могут быть не только из сферы атакованного субъекта. Взаимосвязь и взаимовлияние СКИИ объясняется взаимосвязью сфер деятельности, в которых они функционируют [1, 8, 9].

Деструктивное воздействие на локальном уровне рассматривает воздействие непосредственно на сам СКИИ и его критически важные объекты. Основная проблема анализа деструктов СКИИ заключается в многообразии сфер их деятельности. Определить набор деструктов для каждого объекта КИИ – не сложная задача, в отличии от задачи, связанной с проведением комплексного деструктивного анализа СКИИ.

Образцы и методика эксперимента

Для анализа и оценки деструктивного воздействия на СКИИ используются следующие методы и подходы: сети Петри (моделирующая система CPN Tools); имитационное моделирование; моделирование систем с использованием Марковских случайных процессов; функциональное моделирование; концептуальные карты.

В результате анализа данных методов [10 – 17], в качестве наиболее рациональных определены: сети Петри – для проведения оценки деструктивного воздействия и моделирования работы деструктов, а также функциональное моделирование – для анализа полученных результатов моделирования.

Сети Петри (моделирующая система CPN Tools) – математический аппарат для моделирования динамических дискретных систем. Сеть Петри представляет собой двудольный ориентированный мультиграф, состоящий из вершин двух типов– позиций и переходов, соединённых между собой дугами. В позициях могут размещаться метки (маркеры), способные перемещаться по сети. Событием называют срабатывание перехода, при котором метки из входных позиций этого перехода перемещаются в выходные позиции [10-12]. События происходят мгновенно либо разновременно, при выполнении некоторых условий.

Функциональное моделирование (IDEFO (Erwin)) позволяет описывать любые системы, в том числе информационные, создавать описание системы и ее внешнего окружения до определения окончательных требований к ней [16]. Т.е. с

помощью данной методологии можно постепенно выстраивать и анализировать систему даже тогда, когда трудно еще представить ее воплощение. Основу методологии IDEF0 составляет графический язык описания процессов. Модель в нотации IDEF0 представляет собой совокупность иерархически упорядоченных и взаимосвязанных диаграмм. Каждая диаграмма является единицей описания системы и располагается на отдельном листе.

Для проведения анализа деструктивного воздействия на СКИИ в общем виде на локальном уровне предлагается подход, основанный на исследовании жизненного цикла СКИИ. Стадии жизненного цикла СКИИ: 1. Анализ требований для СКИИ, 2. Проектирование системы защиты СКИИ, 3. Реализация системы защиты СКИИ, 4. Внедрение системы защиты СКИИ, 5. Сопровождение СКИИ, 6. Реорганизация и ликвидация СКИИ.

Исходя из стадий жизненного цикла СКИИ и их особенностей, выделим следующие виды деструктов:

- Destr 1 – ошибки при анализе требований для СКИИ. Исходя из подэтапов первой стадии жизненного цикла СКИИ, возможны следующие ошибки: ошибки в определении критических процессов, ошибки в перечне объектов КИИ, подлежащих категорированию, ошибки при проверке и согласовании перечня объектов, подлежащих категорированию. Однако, в случае корректной проверки перечня объектов КИИ, подлежащих категорированию, и исправлении перечня объектов, данный деструкт станет неактуальным для СКИИ и его воздействие перекроется.
- Destr 2 – ошибки инфраструктурного анализа. Данный деструкт выделен отдельно от основных стадий жизненного цикла СКИИ. Ошибки инфраструктурного анализа могут возникать на стадиях проектирования системы защиты СКИИ и его сопровождения. Инфраструктурный анализ определяет взаимосвязь и взаимовлияние объектов КИИ. Данный деструкт характеризует влияние атаки на объекты КИИ, которые взаимосвязаны с атакованным объектом. Неверный инфраструктурный анализ влияет на оценку рисков реализации атаки. На стадии сопровождения инфраструктурный анализ учитывает изменение количества объектов, что приводит к необходимости повторного прохождения стадий жизненного цикла СКИИ, начиная с первой стадии.
- Destr 3 – ошибки в проектировании системы защиты. Исходя из подэтапов стадии проектирования системы защиты СКИИ, следует выделить следующие возможные ошибки: ошибки в категорировании объектов КИИ, где возможен Destr 2, исходя из ошибок категорирования,

ошибки в формировании перечня требований по обеспечению безопасности значимы объектов КИИ, а также ошибки при формировании мер для перекрывания требований по обеспечению безопасности значимых объектов КИИ.В случае обнаружения ошибок в категорировании и корректного исправления, возможно перекрывание данного деструкта частично, так как исправление ошибок при категорировании не гарантирует отсутствие ошибок в формировании мер для перекрывания требований по обеспечению безопасности значимых объектов КИИ.

- Destr 4 – ошибки при реализации системы защиты СКИИ. На стадии реализации системы защиты СКИИ возможно частичное перекрывание Destr 3, при проверке требований по обеспечению безопасности значимых объектов КИИ, а также мер защиты по перекрыванию данных требований. На данной стадии жизненного цикла СКИИ осуществляется реализация мер по защите СКИИ и тестирование системы защиты СКИИ с последующим ее исправлением. В случае некорректной проверки требований по обеспечению безопасности значимых объектов КИИ и мер защиты по перекрыванию данных требований появляются ошибки в реализации мер защиты СКИИ, то есть ошибки в системе защиты. При реализации системы защиты КИИ возможны ошибки в выполнении и реализации требований и мер защиты СКИИ, даже если система защиты СКИИ была спроектирована верно. Ошибки при тестировании системы защиты СКИИ влекут за собой ошибки в исправлении системы защиты СКИИ. В результате система защиты СКИИ имеет целый ряд уязвимостей, которые могут быть использованы для реализации атак Destr 7.
- Destr 5 – ошибки при внедрении системы защиты СКИИ. Destr 4 влечет за собой Destr 5, то есть внедрение системы защиты СКИИ, в которой имеются неперекрытые уязвимости. В случае корректной системы защиты СКИИ существует возможность ошибок при внедрении системы защиты на всем СКИИ. Также в данный деструкт входят ошибки, связанные с неуведомлением персонала об изменениях защиты и новых правилах реализации системы защиты. Исправление ошибок внедрения возможно при повторном прохождении жизненного цикла в случае, если на стадии сопровождения были обнаружены инфраструктурные изменения, в результате чего произошел переход на стадию 1. В этом случае возможно последующее прохождение стадий жизненного цикла без появления деструктов.

– Destr 6– ошибки при сопровождении СКИИ. Данный деструкт подразумевает Destr 2, в случае ошибок инфраструктурного анализа при изменении количества значимых объектов, подлежащих категорированию. Стадия сопровождения СКИИ реализует возврат на первую стадию жизненного цикла СКИИ, в случае изменения количества объектов КИИ, так как там осуществляется формирование перечня объектов КИИ, подлежащих категорированию. Существует вероятность перекрывания Destr 1 – ошибок при анализе требований.
– Destr 7 – угроза реализации атаки на СКИИ. Данный деструкт реализуется исходя из вышеперечисленных деструктов, особенно в случае ошибок в системе защиты СКИИ (Destr 4), реализованной с неперекрытыми уязвимостями, которые могут быть использованы для реализации атак на СКИИ.

Необходимо отметить, что не обнаружение (или не учет) деструкта на определенном этапе жизненного цикла СКИИ влечет за собой появление новых деструктов в дальнейшем (на последующих этапах). При этом можно определить значения таких показателей, как «уровень критичности деструкта» и «уровень критичности СКИИ».

Исходя из того, что возможность реализации каждого деструкта, за исключением Destr 7, зависит от конкретной стадии жизненного цикла СКИИ, которую проходит отдельно взятый субъект, для анализа оценки деструктивного воздействия на СКИИ предлагается математическая модель в дискретном времени.

Для оценки деструктивного воздействия выделены следующие параметры:

– Param1 – стадия жизненного цикла СКИИ, на которой появляется деструкт.
– Param2 – время жизни Destr, в случае, если деструкт не обнаруживается в жизненном цикле СКИИ.
– Param3 – условия устранения деструкта.
– Param4 – время жизни Destr, в случае, если на каком-либо этапе жизненного цикла деструкт обнаруживается и устраняется.
– Param5 – порождение дополнительных деструктов.

Для каждого деструкта собирается отдельная модель при помощи сетей Петри, оцениваемая по параметрам. На рисунке 1 представлена модель оценки деструктивного воздействия на СКИИ для Destr 1 «ошибки при анализе требований для СКИИ», собранная в программе CPN Tools.

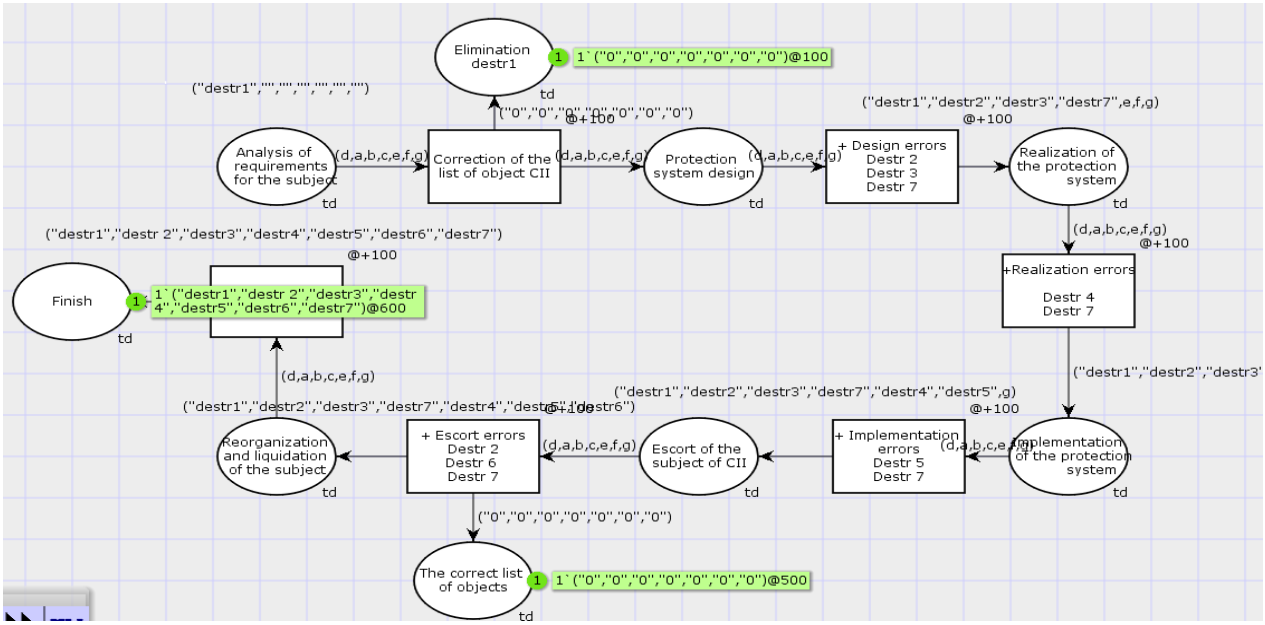

Рисунок 1 – Моделирование действия Destr 1

Модель воспроизводит сценарий зарождения Destr 1 на первой стадии жизненного цикла СКИИ с последующим прохождением всех остальных стадий. В модели учтены условия перекрывания Destr 1 на первой стадии жизненного цикла СКИИ, в случае корректировки списка объектов КИИ, подлежащих категорированию, а также на пятом этапе жизненного цикла СКИИ – сопровождение СКИИ в случае, если произошли инфраструктурные изменения.

Результаты и обсуждение

Анализ результатов экспериментального исследования показал, что наиболее критичная стадия жизненного цикла СКИИ – анализ требований для СКИИ. В случае возникновения ошибок на первой стадии жизненного цикла СКИИ, т.е. появление Destr 1, появление остальных деструков, а также уязвимостей, увеличивающих вероятность реализации атак на СКИИ, неизбежно. Вторым деструктом по уровню влияния на СКИИ является Destr 2 – ошибки инфраструктурного анализа. Анализ показал взаимосвязь появления деструктов от реализации других деструктов (рисунок 2). Модель IDEF0 наглядно демонстрирует взаимосвязь и взаимовлияние деструктов, в результате чего в системе СКИИ появляются уязвимости, которые могут быть использованы злоумышленниками для реализации атак – Destr 7.

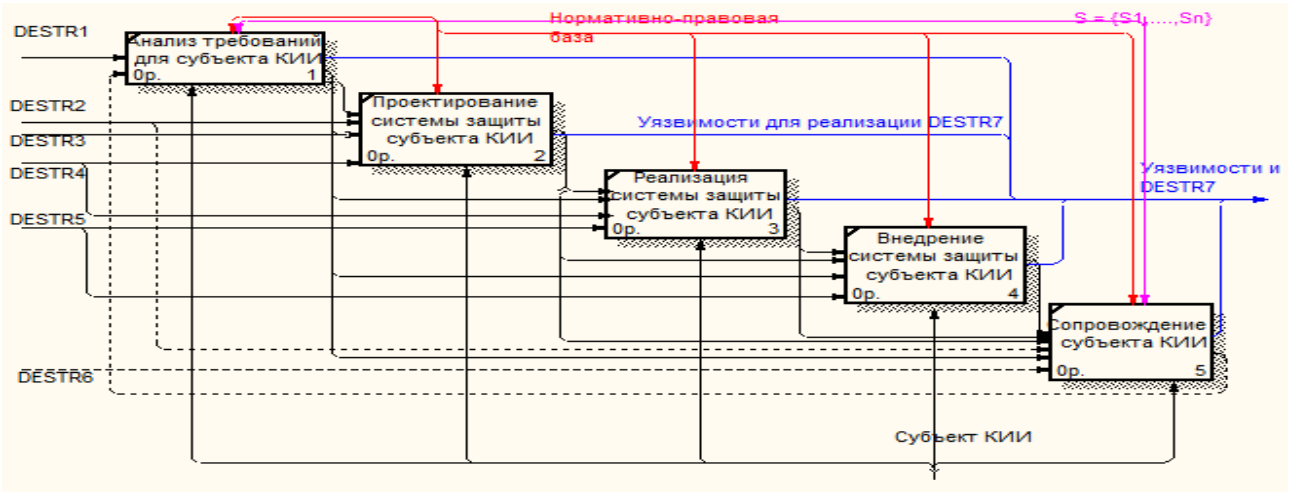

Рисунок 2 – Модель IDEF0, отражающая взаимовлияние (последействие) деструктов на стадиях жизненного цикла СКИИ

В процессе проведения экспериментального исследования, один из значимых параметров для оценки деструктивного воздействия на СКИИ- время жизни деструктов в процессе жизненного цикла СКИИ. Данный параметр представляет собой время в единицах программного времени, за которое деструкт пройдет все стадии жизненного цикла (рисунок 3).

Реализация некоторых деструктов возможна с двух стадий, что было также учтено при оценки данного параметра. Наиболее «живучим» является Destr 1, а также, при определенных условиях возникновения, Destr 2, Destr 3, Destr 4.

Рисунок 3 – Диаграмма времени жизни деструктов в процессе жизненного цикла СКИИ

В ходе экспериментального исследования выявлены условия устранения деструктов и время, которое необходимо для их обнаружения и устранения. В результате стало возможным сравнение времени жизни деструкта в процессе жизненного цикла СКИИ, со временем, необходимым для его устранения (рисунок 4). В случае с Destr 1, Destr 3 и Destr 4 стоит отметить, что возможное время их устранения гораздо меньше, чем время их воздействия до конца жизненного цикла СКИИ. Однако, следует обратить внимание на такие деструкты, как Destr 2, Destr 5 и Destr 6. Наибольшая опасность их воздействия заключается в том, что время, необходимое на их исправление гораздо больше, чем время жизни до конца жизненного цикла СКИИ. Т.е. возможность обнаружить и нейтрализовать воздействие данных деструктов существует только при повторном прохождении жизненного цикла СКИИ. Большое значение времени обнаружения и устранения увеличивает вероятность успешной реализации атак злоумышленниками, которые могут использовать уязвимости СКИИ.

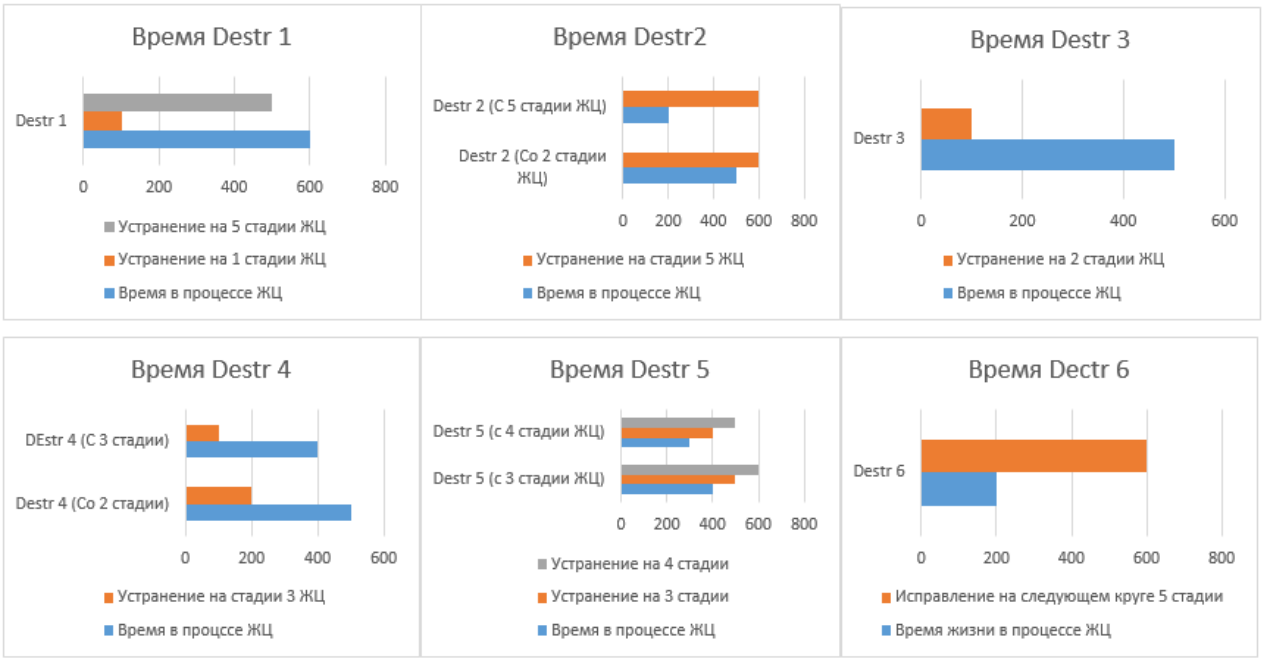

Рисунок 4 – Распределение времени деструктов на стадиях жизненного цикла СКИИ

В результате анализа функциональной модели IDEF0 (рисунок 2), выведена следующая функция взаимозависимости деструктов:

$$Destr6 = Destr6(Destr5(Destr4(Destr3(Destr2\ (Destr1)))) \quad (1)$$

Исследование полученной функциональной модели (рисунок 2) и функции зависимости деструктов (1) позволило определить шкалу оценки уровня критичности деструктивного воздействия на СКИИ. Под уровнем критичности в данном случае будем понимать уровень негативного воздействия, который характеризует появление уязвимостей в СКИИ.

Шкала оценки уровня критичности деструктивного воздействия на СКИИ:

- 1-уровень критичности – самый высокий уровень отрицательного воздействия, который появляется в результате воздействияDestr 1, так как согласно функции зависимости от Destr 1 зависят остальные деструкты.
- 2-уровень критичности –уровень, характеризующийся воздействием Destr2.
- 3-уровень критичности – характеризуется воздействием Destr 3.
- 4-уровень критичности – воздействие Destr 4.
- 5-уровень критичности – воздействие Destr 5.
- 6-уровень критичности – воздействие Destr 6.

Введение данной шкалы позволит комплексно оценить деструктивное воздействие на СКИИ без привязки к конкретной сфере функционирования субъекта, решить проблему оценки деструктивного воздействия на СКИИ на локальном уровне. В случае возникновения инцидента информационной безопасности, после определения уязвимости, которая способствовала реализации атаки, шкала поможет определить уровень критичности деструктивного воздействия на СКИИ.

Заключение

Исследование жизненного цикла СКИИ позволило определить 6 видов деструктов инфраструктурного характера. Для экспериментального исследования выделены параметры оценки деструктивного воздействия на СКИИ. По выделенным параметрам оцениваются и сравниваются модели действия деструктов на сетях Петри.

Экспериментальное исследование показало, что существует зависимость активации реализации одних деструктов от других. Наиболее опасным деструктом является Destr 1, так как он активирует появление всех остальных деструктов и имеет наибольшее время жизни в процессе жизненного цикла СКИИ. Следовательно, стадия «Анализ требований для СКИИ» жизненного цикла СКИИ является наиболее ответственной и важной для последующего функционирования СКИИ.

В ходе экспериментального исследования определены условия устранения деструктов и время, необходимое на обнаружение и устранение деструкта. Как показал анализ результатов экспериментального исследования, наиболее долгим временем обнаружение и устранение обладают Destr 2, Destr 5 и Destr 6, что подчеркивает необходимость наиболее частых и внимательных проверок системы безопасности СКИИ. Destr 2 – ошибки инфраструктурного анализа, второй деструкт по степени критичности деструктивного воздействия на СКИИ, который может возникнуть на двух стадия жизненного цикла КИИ: «Проектирование системы защиты СКИИ» и «Сопровождение СКИИ», что подчеркивает необходимость более тщательного и внимательного инфраструктурного анализа СКИИ.

Введенная шкала оценки деструктивного воздействия на СКИИ, определяет комплексный подход к оценке и позволяет определить уровень критичности деструктивного воздействия на СКИИ, в случае возникновения инцидента информационной безопасности.

Библиографический список

1. О безопасности критической информационной инфраструктуры Российской Федерации : Федер. закон от 26.07.2017 № 187-ФЗ. – URL: http://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 13.03.2020).
2. Critical Information Infrastructure : site. – URL: https://publicwiki-01.fraunhofer.de/CIPedia/index.php/Critical_Information_Infrastructure#cite_note-70 (accessed: 15.03.2020).
3. Presidential directive PDD-63 22 may 1998. – URL: https://fas.org/irp/offdocs/pdd/pdd-63.htm (accessed: 14.03.2020).
4. О европейских критических инфраструктурах и мерах по их защите : Директива Совета Европейского Союза 2008/114/ЕС от 8 дек. 2008 г. – URL: https://base.garant.ru/70333008/ (дата обращения: 14.03.2020).
5. Лукацкий. А. Статистика реальных инцидентов ИБ в индустриальных системах / А. Лукацкий // Securitylab. – URL: https://www.securitylab.ru/blog/personal/Business_without_danger/38672.php (дата обращения: 20.03.2020).
6. Актуальные киберугрозы 2019 года. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-q1-2019/#id3 (дата обращения: 20.03.2020).
7. Деструктивное воздействие // Википедия : свобод. энцикл. – URL: https://ru.wikipedia.org/wiki/Деструктивное_воздействие (дата обращения: 21.03.2020).
8. Common Threats and Vulnerabilities of Critical Infrastructures / Rosslin John Robles1 , Min-kyu Choi1, Eun-suk Cho [et al.] // International Journal of Control and Automation. – P. 17–22. – URL: http://article.nadiapub.com/IJCA/vol1_no1/3.pdf (accessed: 14.03.2020).

9. Информзащита. Системный интегратор: Федер. закон № 187-ФЗ. – URL: https://infosec.ru/glavnye-temy/187-fz/ (дата обращения: 22.03.2020).
10. Питерсон. Дж. Теория сетей Петри и моделирование систем / Дж. Питерсон. – Москва : Мир, 1984. – 264 с.
11. Котов В. Сети Петри / В. Котов. – Москва : Наука, 1984. – 160 с.
12. Сети Петрию // Википедия : свобод. энцикл. – URL: https://ru.wikipedia.org/wiki/Сети_Петри (дата обращения: 23.03.2020).
13. Имитационное моделирование // Википедия : свобод. энцикл. – URL: https://ru.wikipedia.org/wiki/Имитационное_моделировние (дата обращения: 25.03.2020).
14. Лычкина. Н. Н. Имитационное моделирование экономических процессов : учеб. пособие / Н. Н. Лычкина. – Москва : ИНФРА-М, 2013. – 254 с. – URL: http://simulation.su/uploads/files/default/2005-uch-posob-lychkina-1.pdf (дата обращения: 26.03.2020).
15. Моделирование систем с использованием Марковских случайных процессов. – URL: http://kopilka77.ru/docs/gsv/disciplini/model/L3.pdf (дата обращения: 26.03.2020).
16. Методология IDEF0. – URL: https://www.sites.google.com/site/anisimovkhv/learning/pris/lecture/tema6/tema6_2 (дата обращения: 27.03.2020).
17. Новые информационные технологии для тебя. Концептуальные карты или концепт-карты. – URL: https://nitforyou.com/konceptualnye-karty/ (дата обращения: 28.03.2020).