DOI 10.37882/2223-2966.2023.6-2.02

ТАКСОНОМИЯ КИБЕРАТАК ПРОЦЕССА ОБРАБОТКИ И ПЕРЕДАЧИ ИНФОРМАЦИИ НА АЭС

TAXONOMY OF CYBER ATTACKS OF INFORMATION PROCESSING AND TRANSMISSION AT NPPS

S. Arvanova

Summary: In general, the IT taxonomy is not suitable for the purposes of nuclear regulation. In particular, it is necessary to restore security related to nuclear security issues. For this reason, the taxonomy for nuclear power plants includes attack procedure, attack vector, attack consequences, vulnerability, and countermeasures. The systems used in nuclear power plants cannot update their security system attack lists via the worldwide network. This means that a taxonomy of cyber attacks for nuclear power plants is needed.

Keywords: nuclear power, cyber security, taxonomy of cyber attacks, digital computer systems, digital communication systems.

Арванова Саният Мухамедовна
Аспирант,
Южный федеральный университет, г. Таганрог;
старший преподаватель,
Кабардино-Балкарский государственный университет им. Х.М. Бербекова, г. Нальчик
sani_07@mail.ru

Аннотация: В целом, таксономия в области ИТ не подходит для целей регулирования в ядерной сфере. В частности, необходимо восстановить безопасность, связанную с вопросами ядерной безопасности. По этой причине таксономия для АЭС включает в себя процедуру атаки, вектор атаки, последствия атаки, уязвимость и контрмеры. Системы, используемые на АЭС, не могут обновлять списки атак своей системы безопасности через мировую сеть. Это означает, что необходима таксономия кибератак для АЭС.

Ключевые слова: ядерная энергетика, кибербезопасность, таксономия кибератак, цифровые компьютерные системы, цифровые коммуникационные системы.

С развитием цифровых контрольно-измерительные приборов и автоматики (КИПиА) устройств кибербезопасность на атомных электростанциях (АЭС) стала актуальной проблемой. Атака Stuxnet, уничтожившая в 2010 году иранский объект по обогащению урана, позволяет предположить, что кибератаки на АЭС могут даже привести к аварии с выбросом радиоактивных материалов.

Однако исследования кибербезопасности промышленных систем управления (ICS) и систем диспетчерского контроля и сбора данных (SCADA) относительно недостаточны по сравнению с информационными технологиями (IT), и в дальнейшем трудно изучить таксономию кибератак для АЭС, учитывая особенности ICS. Передовые исследования таксономии кибератак не отражают архитектурные и внутренние характеристики АЭС и не имеют систематической стратегии противодействия, поэтому необходимо более систематически проверять согласованность действий операторов и регулирующих органов в отношении кибербезопасности, согласно требованиям в руководстве по регулированию 5.71 (RG.5.71) и стандарте регулирования 015 (RS.015).

Устройства КИПиА атомных электростанций (АЭС) переходят от аналоговых устройств к цифровым, поскольку аналоговые устройства КИПиА имеют относительно низкую производительность и трудности в обслуживании [1]. Цифровые КИПиА, применяемые на АЭС, должны соответствовать лицензионным требованиям по безопасности, а кибербезопасность является наиболее важным вопросом [1, 2].

Согласно отчету Группы реагирования на чрезвычайные ситуации в киберпространстве (ICS-CERT), уязвимость промышленных систем управления и систем диспетчерского контроля и сбора данных продолжает расти. Система диспетчерского контроля и сбора данных может дистанционно контролировать и управлять системой на большой территории, например, газо-/нефтепроводами и системами электропередачи, а промышленные системы управления включат все типы систем промышленной автоматизации, в том числе распределенные системы управления (DCS), которые распределяют подсистемы блока управления по группам блоков. АЭС является репрезентативным объектом системы ICS и SCADA. В отчете ICS-CERT также сообщается о кибератаках и нарушениях кибербезопасности, направленных на системы ICS и SCADA [3]. Показательной кибератакой на ядерный объект является Stuxnet, который физически уничтожил центрифуги иранского предприятия по обогащению урана. Кроме того, АЭС Davis-Besse в США была атакована вирусом Slammer, что привело к неработоспособности системы индикации состояния безопасности на 5 часов. В Корее компьютерная сеть компании Korea Hydro & Nuclear Power (KHNP) подверглась атаке в результате которой злоумышленник забрал проект и руководство АЭС, а также личную информацию сотрудников.

Для предотвращения и реагирования на киберугрозы в ситуациях, когда киберугрозы возрастают, необходимо выбрать прогнозируемые кибератаки на АЭС и оценить соответствие кибербезопасности цифровых устройств, которые могут гарантировать надёжность и производительность [4, 5]. Для прогнозирования кибе-

ратак на АЭС и оценки соответствия кибербезопасности необходимо провести исследования случаев кибератак на основе таксономии кибератак, которая отражает характеристики АЭС. Однако существует недостаток исследований по систематической таксономии кибератак, которая бы отражала характеристики АЭС.

В данной работе предлагается таксономия кибератак, которая отражает такие характеристики АЭС, как процедура атаки, вектор атаки, последствия атаки, уязвимость и контрмеры. Кроме того, в качестве примера кибератаки (например, смертельный пинг (Ping of Death) — DDoS-атака, при которой злоумышленник предпринимает попытки завершить работу системы, дестабилизировать или заморозить целевой компьютер или службу, отправляя неправильно сформированные или пакеты большого размера с помощью простой команды пинг), представлен шаблон таксономии, состоящий из предложенных элементов таксономии.

Характеристики таксономии на АЭС

Для того, чтобы выполнить все необходимые испытания функций безопасности и верификацию цифровых устройств КИПиА, которые будут применяться на АЭС, необходимо провести анализ кибератак на основе систематической таксономии. Передовые исследования таксономии кибератак в основном относятся к области информационных технологий (ИТ), а таксономия, относящаяся к ICS и SCADA, фокусируется на понятии угрозы. Однако, по мере роста кибератак на системы ICS и SCADA, появляются исследования таксономии, сфокусированные на самой кибератаке. Кроме того, исследования таксономии проводятся для конкретных объектов, таких как энергетические станции. Некоторые из этих исследований рассматриваются ниже.

Хансман [6] предложил четырёхступенчатую категоризацию компьютерных и сетевых атак на основе класса атаки, цели атаки, уязвимостей и полезной нагрузки. Класс атаки — это вектор атаки, который классифицирует большую категорию кибератак в соответствии с методом атаки. Например, уровень 1 — взлом пароля, уровень 2 — атака на угадывание и уровень 3 — атака методом перебора. Для цели атаки объект кибератаки подробно описывается как класс атаки. Например, цель атаки подразделяется на большие категории, такие как аппаратное обеспечение на уровне 1, компьютер на уровне 2, сетевое устройство на уровне 3 и коммутатор на уровне 4. Для уязвимостей используется Common Vulnerabilities and Exposures (CVE).

Уязвимость Говарда [6, 7] использовалась для уязвимостей в реализации, проектировании и конфигурации. Полезная нагрузка атаки делится на утечку информации, разрушение и невозможность обслуживания.

Флери [8] предложил модель «атака–уязвимость–ущерб» (AVD), в которой рассматриваются способы атаки на систему управления, последствия атаки, способы реагирования на атаку и требования к механизму защиты. Атака — представляет собой цель атаки, источник атаки и метод атаки. Уязвимость — фокусируется на причине успеха конкретной атаки и слабости системы. Ущерб — связан с тяжестью атаки.

Таксономия Симмонса [9] предлагает модель системы классификации кибератак под названием AVOIDIT с учетом вектора атаки, оперативного воздействия, защиты, информационного воздействия и цели атаки. Вектор атаки — это уязвимость и путь для атаки.

Оперативное воздействие — это эффективность атаки на работу системы. Защита — это фаза смягчения последствий атаки. Информационное воздействие представляет собой влияние на информацию, например, утечки и изменения. Цель атаки — это объект атаки, например, система или сеть.

К. Харрисоном и Дж.Уайтом [10] предложена таксономия, которая учитывает уязвимость отдельной системы и влияние кибератак на сообщество. Таксономия Уайта в основном классифицируется на вершины событий и векторы последствий. Вектор события описывает источник кибератаки, цель атаки и описание кибератаки, связанное с методом и уязвимостью. Вектор последствий описывает сектор общества, пострадавший от кибератаки, причину воздействия и метрики оценки воздействия.

М.Б. Лайн, А. Занд, Г. Стрингини [11] сосредоточились на характеристиках целевых атак и классифицировал категории в соответствии с целью атаки, начальным вектором атаки, боковым перемещением и положением командно-контрольного сервера. Цель атаки — это буквально предполагаемая цель попытки кибератаки. Начальный вектор атаки — это путь атаки. Боковое перемещение — это то, как атака действует после заражения системы. Положение командно-контрольного сервера определяет, как можно попытаться вторгнуться снова.

С.К. Смит, А. Олтрамари [12] сосредоточились на самом случае с помощью матрицы, основанной на событиях, и предложили систему классификации на основе целевой отрасли, местоположения, типа вредоносного ПО и типа атакующего.

В работе авторов Д. Папп, З. Ма, Л. Бутян [13] проанализированы атаки и уязвимости встраиваемых систем. Университет Карнеги-Меллон принял во внимание поведение человека, сбои системы, ошибки внутреннего процесса и внешние события для оценки рисков кибербезопасности при эксплуатации системы. Исследования

по таксономии кибератак в основном сосредоточены на сети и не затрагивают архитектурные характеристики таких систем, как АЭС. Архитектурные характеристики — это проектная структура объекта. В случае типичных АЭС в Корее, система защиты реактора (RPS) имеет четыре программируемых логических контроллера (PLC) в логике 2-out-of-4, так что даже если один PLC будет выведен из строя в результате кибератаки, это не представляет угрозы для нормальной работы АЭС. Это означает, что для того, чтобы повлиять на работу АЭС, необходимо вывести из строя три или четыре программируемых логических контроллера путём одновременного проведения кибератаки на них. Нецелесообразно рассматривать серьезность и меры противодействия кибератакам без изменения архитектурной структуры АЭС. Поэтому в данной статье рассматриваются архитектурные характеристики АЭС и предоставляется информация, которую необходимо учитывать для обеспечения кибербезопасности АЭС.

Кроме того, в отличие от общих ИТ и ИКС, на АЭС существуют риски утечки радиоактивного излучения и незаконной передачи ядерных материалов. Чтобы защитить АЭС от этих рисков, АЭС имеют различные характеристики по сравнению с ИТ и ИКС. В статье рассматриваются такие характеристики АЭС, как стратегия «защита в глубину», время простоя реактора и возможность утечки радиоактивных материалов в случае серьезной аварии. Кроме того, предлагаются систематические стратегии для согласования контрмер с векторами атак и последствиями атак, которые не рассмотрены в предыдущих исследованиях. Кроме того, характеристики кибератак и соответствующие контрмеры сопоставлены с характеристиками Regulatory Guide 5.71 (RG.5.71) [14], нормативного руководства по программам кибербезопасности для ядерных объектов, для проверки соответствия контролю безопасности при внедрении цифрового оборудования на АЭС.

Как упоминалось выше, категории таксономии сгруппированы в соответствии с определёнными понятиями. Путём увеличения случаев кибератаки с использованием шаблонов, сделанных из предложенных категорий таксономии, они могут быть использованы в качестве данных для проверки соответствия цифровых устройств КИПиА, которые будут применяться на АЭС. Эти данные также могут быть использованы в качестве эффективных стратегий противодействия кибератакам. Для этих целей в качестве категорий таксономии предлагаются процедура атаки, вектор атаки, последствия атаки, контрмеры и уязвимость.

Схема классификации этапов для таксономии кибератак представлена на рисунке 1.

Целью предлагаемой таксономии является разработка стратегических контрмер, воздействующих на последствия атак и векторы атак, а также использование для тестирования соответствия.

Чтобы продемонстрировать эффективность таксономии, предлагается контрмера, когда система мониторинга предприятия (PMS) подвергается атаке «пинг смерти», и объясняется, как использовать таксономию в тесте на соответствие. Прежде чем показать контрмеры, следует отметить, что контрмеры, связанные с PMS, представленные в этой статье, предназначены для представления использования таксономии, которая является сценарием, учитывающим только основные функции PMS. Фактические методы связи и характеристики конструкции не представлены в сценарии в качестве элемента безопасности, и они могут отличаться от фактических сценариев реагирования. PMS имеет возможность рассчитать, какую группу элементов управления выбрать для системы быстрого отключения питания (СБПВ). Хотя она не нацелена на непосредственное управление, она выполняет функции, связанные с механизмами приведения в действие управляющих стержней. Поэтому последствия кибератаки могут повлиять на функции системы быстрого отключения питания. PMS состоит из системы сбора данных станции (PDAS) и компьютерной системы станции (PCS). PDAS отвечает за передачу входных переменных станции в PCS. PCS обрабатывает, вычисляет, предупреждает и сохраняет входные переменные, полученные от PDAS, и информирует оператора через другие системы, расположенные рядом с PCS. Если «пинг смерти» используется в PCS инсайдером или вредоносным ПО, PDAS не может выполнять свои функции из-за большого количества пакетов, что может привести к тому, что PCS не сможет получить входные переменные установки. В качестве контрмеры для этого может быть применена защита в глубину, которая определяет PCS как более высокий класс, чем PDAS, для обмена данными. Стратегия «защита в глубине» — это способ предотвратить прохождение сигналов и данных от низкоклассного ЦДА к высококлассному ЦДА, хотя высококлассный ЦДА может отправлять данные на низкоклассный ЦДА. Это может быть контрмерой для предотвращения передачи сигнала смерти от PCS к PDAS. Кроме того, учитывая основные проектные характеристики безопасности АЭС, такие как разнообразие, избыточность и независимость, PDAS должна работать, даже если PDAS1 выйдет из строя. Кроме того, кибератаки можно предотвратить, рассматривая пинг смерти с помощью вектора атаки (Использование неполной сети) и контроля безопасности («Доступ к сети», «Защита от отказа в обслуживании»). В качестве подробной контрмеры для вектора атаки и контроля безопасности, необходимо исследовать подключенную сеть, чтобы исключить неиспользуемую сеть внутри АЭС, и установить уровень безопасности в соответствии с коммуникационной информацией, обмениваемой через сеть. Кроме того, необходимо определить пути связи, прямо или косвенно связанные с CDA, и обе-

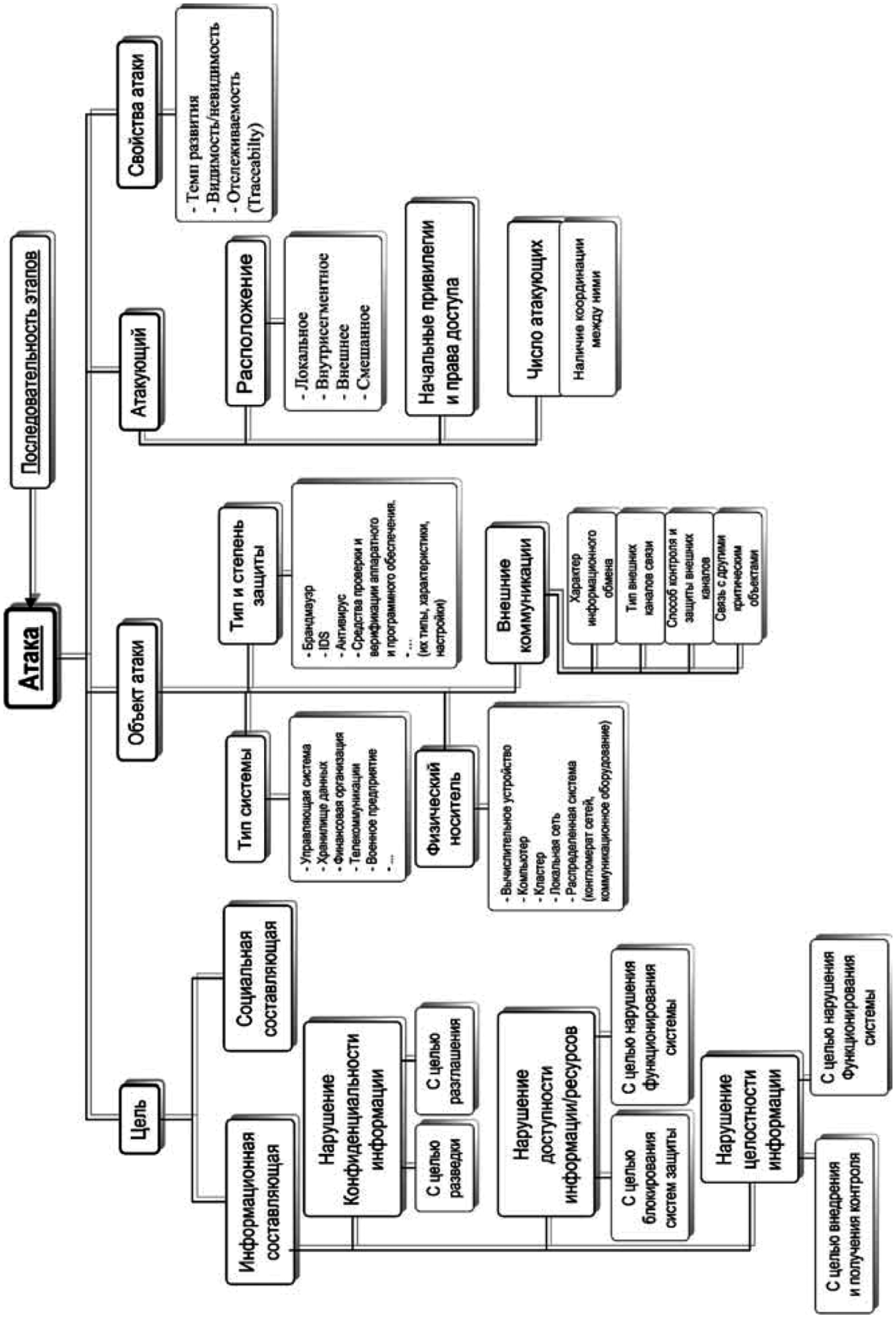

Рис. 1. Классификация этапов для таксономии кибератак

спечить целостность и конфиденциальность передаваемой информации. Сетевой протокол сетевой протокол не должен инициировать команды за пределами одного сетевого диапазона, а команды в сетевом протоколе не должны быть направлены на снижение уровня безопасности требуемых цифровых активов. Перед применением исправлений и обновлений программного обеспечения следует проверить их влияние на безопасность [15].

Ниже описано, как предложенная таксономия может быть применена к тесту соответствия. В основном она оценивает и сертифицирует безопасность и надежность продуктов защиты информации с использованием общих критериев системы. В случае АЭС вместо СС используются RG 5.71 и RS 015, а верификация осуществляется посредством тестирования на проникновение после тестирования на основе документов. Проверка на основе документов — это проверка соответствия средств контроля безопасности, представленных в стандартах безопасности, требованиям к конструкции безопасности цифровых устройств.

Заключение

Предложенная таксономия кибератак учитывает характеристики АЭС. В целом, таксономия в области ИТ не подходит для целей регулирования в ядерной сфере. Но поможет в разработке модели угрозы и мер по предотвращению таких угроз.

Процедура атаки подразделяется на сбор информации, получение прав доступа, командование и управление, а также действия и экзекуцию. Процедура атаки может быть использована в качестве критерия для простоты систематического расследования случаев кибератак. Вектор атаки делится на физический доступ и сетевой доступ. Последствия кибератаки классифицированы как атака, влияющая на функцию системы быстрого отключения питания. Последствия кибератак, влияющих на функцию системы быстрого отключения питания, разделены на саботаж и несанкционированное удаление ядерных материалов. Это можно использовать в качестве основных данных для количественной оценки риска кибератаки.

Тестирование на проникновение позволяет убедиться в том, что контроль безопасности цифровых устройств соответствует рекомендованным нормативным требованиям. Однако существует проблема, при которой для проведения тестирования на проникновение будут использоваться кибератаки. Эта проблема может быть решена с помощью таксономии, представленной в данной статье. Во-первых, применяемые цифровые устройства должны отвечать требованиям стандартов безопасности и соответствовать проектной документации по безопасности цифрового оборудования. В настоящее время, если эти два требования не совпадают, оборудование находится в соответствие верификации на основе документов. Если оба требования выполнены, можно выбрать соответствующую таксономию кибератаки, которая включает элемент контроля безопасности стандартов безопасности. Если кибератака с нормативными директивами применяется непосредственно к оборудованию, а функционирование и работа не нарушаются, оборудование считается прошедшим как тест на основе документов, так и тестирование на проникновение.

ЛИТЕРАТУРА

1. P.A. Khand, «Attack Tree Based Cyber Security Analysis of Nuclear Digital Instrumentation and Control Systems» the Nucleus, vol. 46, 2009, pp. 415-428, 4.
2. D.Y. Kim, Cyber security issues imposed on nuclear power plants, Ann. Nucl. Energy 65 (2014) 141–143.
3. Charles McLellan, Cyberwar and the future of cybersecurity. http://www. zdnet.com/article/cybersecurity-predictions-for-2016-how-are-they-doing/.
4. J. Shin, H. Son, G. Heo, Cyber security risk evaluation of a nuclear I&Co using bn and et, Nucl. Eng. Technol. 49 (3) (2017) 517–524.
5. C.K. Lee, Trend of technology of instrumentation and control system in nuclear power plants, Rev. KIISC 22 (5) (2012) 28–34.
6. S. Hansman, A Taxonomy of Network and Computer Attack Methodologies, 2003.
7. S. Hansman, R. Hunt, A taxonomy of network and computer attacks, Comput. Secur. 24 (1) (2005) 31–43.
8. T. Fleury, H. Khurana, V. Welch, Towards a taxonomy of attacks against energy control systems, in: International Conference on Critical Infrastructure Protection, Springer, Boston, MA, 2008, pp. 71–85.
9. C. Simmons, C. Ellis, S. Shiva, D. Dasgupta, Q. Wu, AVOIDIT: a cyber attack taxonomy, in: Proc. Of 9th Annual Symposium on Information Assurance— ASIA, vol. 14, 2009.
10. K. Harrison, G. White, A taxonomy of cyber events affecting communities, in: System Sciences (HICSS), 44th Hawaii International Conference on, 2011, pp. 1–9.
11. M.B. Line, A. Zand, G. Stringhini, R. Kemmerer, Targeted attacks against industrial control systems: is the power industry prepared?, in: Proceedings of the 2nd Workshop on Smart Energy Grid Security, 2014, pp. 13–22.
12. A.S. Flowers, S.C. Smith, A. Oltramari, Security taxonomies of industrial control systems, in: Cyber-security of SCADA and Ther Industrial Control Systems, 2016, pp. 111–132.
13. D. Papp, Z. Ma, L. Buttyan, Embedded systems security: threats, vulnerabilities, and attack taxonomy, in: Privacy, Security and Trust (PST), 2015 13th Annual Conference on, 2015, pp. 145–152.
14. U.S. NRC, Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, 2010.
15. I.S. Koo, K.W. Kim, S.B. Hong, G.O. Park, J.Y. Park, Digital asset analysis methodology against cyber threat to instrumentation and control system in nuclear power plants, J. Korea Inst. Electron. Commun. Sci. 6 (6) (2011) 839–847.

Журнал «Современная наука: актуальные проблемы теории и практики»