3. Насриддинов К. Элементар зарралар физикаси бўлимини фанлараро алоқадорлик асосида ўқитиш. //” Педагогик таълим”. 2011, № 6. 43-48-б.
4. Наумов А.И. Физика атомного ядра и элементарних частиц. -М.: «Просвещение», 1984. –С.384.
5. Шпольский Э.В. Атомная физика. -Т.1. -М.: “Наука”, 1983. –С. 444.

РЕЗЮМЕ

Ушбу мақолада “Элементар зарралар” физикаси бўлими ўрганадиган жараёнлар ва объектлар фанлараро алоқадорлик тамойили асосида қараб чиқилган

РЕЗЮМЕ

В данной статье изучены процессы и объекты раздела физики элементарных частиц на основе принципа межпредметной связи

SUMMARY

In the article Elementary particle Physics processes and objects are studied on the basis of the inter subject principle

INFORMATION SECURITY STAGES OF THE INTEGRATION OF ALTERNATIVE ENERGY SOURCES IN THE GENERAL ELECTRICAL NETWORK

S.R.Davronov - *doctoral student*

Karshi state university

Tayanch so'zlar: integratsiya, axborot xavfsizligi, jarayonlarni boshqarishning avtomatlashtirilgan tizimi, baholash obyekti, identifikatsiya, zaiflik, aktivlar, kiber-xavfsizlik, dasturiy ta'minot.

Ключевые слова: интеграция, информационная безопасность, АСУ ТП, объект оценки, идентификация, уязвимость, активы, кибербезопасность, програмное обеспечение.

Key words: integration, information security, automated process control system, object of assessment, identification, vulnerability, assets, cyber security, software.

The development of technology in the energy sector, has started such a thing as smart network, but to create such a network it is necessary to integrate various sources of electricity in one managed network. So to solve the problem of the integration of scientists of many countries are conducting studies in the field of integration of alternative energy sources in the general electrical network. But one of the main aspects of integrated networks are to ensure information security. Since to find a solution to the integration and providing it information security is a priority task. According to the Decree of the President No. PP-4422 (August 22 2019 bringing the share of renewable energy sources by 2030 to more than 25 percent of the total electricity generation [1]. The table below shows the further development of renewable energy sources:

№	The name of indicators	Forecast for an increase in generating capacity, MW					The share of electricity generation, %	
		2019 г.	2020 г.	2021 г.	2022 г.	2023 — 2030 гг.	2018 г.	2030 г.
Total		**1074,1**	**886,8**	**1 961,5**	**2 061,6**	**14 017,8**	**100**	**100**
1.	Traditional energy	1 050	1 807	1 777	2 259,4	10 910,2	90	75
	including capacity withdrawal	-	1 060	320	740	4 280	-	-
2.	Renewable energy sources	24,1	119,8	504,5	542,2	7 387,6	10	25
	of them:							
2.1.	Hydropower	24,1	119,8	204,5	42,2	1 487,6	10	11,2
2.2.	Solar power	-	-	300	400	4 300	-	8,8
2.3.	Wind power	-	-	-	100	1 600	-	5

Table 1. Further development of renewable energy sources

As in Figure 1, you can see the installed capacity of solar energy by 2030 will be 4,300 MW. The installation of large-capacity solar power plants requires their connection to a common electric grid. Thus, the connection of solar power plants to a common network and their remote control require certain solutions to ensure information security in the management of electric networks.

Technology management of hybrid networks emanate from the notion of intellectual networks (Smart Grid), which is used in the integration of renewable energy in centralized energy network, called the hybrid network. This technology provides the flexibility of the network and will manage all processes in the network and provide uninterrupted supply of electricity to the end user [2]. Also, the International Institute of electrical and Electronics Engineers (IEEE) give the following definition: "a fully integrated, self-regulating and self-healing power system network topology and incorporating assume all generating sources, main and distribution networks and all types of consumers of electric energy, managed a single network of automated devices in real time "[3]. In terms of national energy technology laboratory (NETL) United States: "the Smart Grid-a set of organizational changes, new process model, information technology solutions, as well as innovations in the field of APCS and dispatching management in the electricity industry"[4].

Integrated network with above mentioned capabilities needed in information security, as the electrical network with such capability is strictly protected infrastructure of any State and its security is considered a priority. Ensuring the security of such systems have performed in phases, based on the international standards for security.

Security begins with the identification of vulnerabilities as specified in the international standard ISO/IEC 27001, you need to identify vulnerabilities that can be exploited, for damage [6].

Vulnerability identified in the following areas:

- Organization of work;
- processes and procedures;
- established norms of governance;
- staff;
- physical environment;
- configuration of the information system;
- hardware, software and communications equipment;
- dependency on external parties.

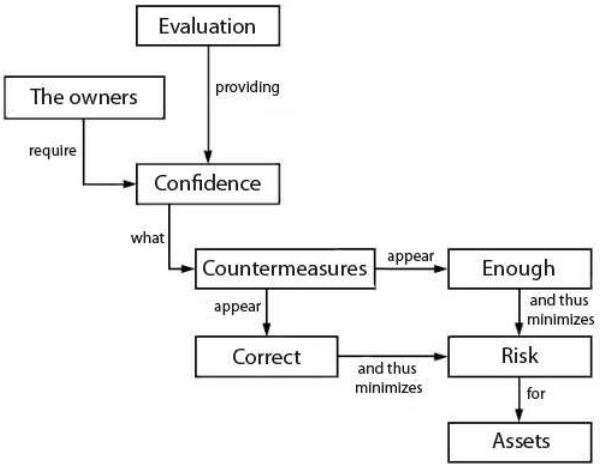
The presence of a vulnerability is not harmful in itself, until used. The vulnerability that has no corresponding threats may not require controls but occasionally must be monitored for measurements. It should also be noted that improperly implemented or incorrect functioning monitoring tool the means of control, which does not itself is used incorrectly can be a vulnerability. Means of monitoring can be effective or ineffective, depending on environment in which it operates.

Also after identify vulnerabilities, you must define the evaluation object (EO).

EO is define as a set of software, hardware and software and/or hardware, possibly accompanied by guides. Regarding ISO/IEC 15408 better balance between EO and any product IT is important only in one aspect: evaluation of EO, containing part of the product, IT should not be mistaken to represent both an evaluation of the product as a whole, IT [7]. Also (picture 1) describes the concepts used in the valuation and their interrelationships.

Examples of EO are [7]:

- program application;
- operating system;
- application program in conjunction with the operating system;
- application program in conjunction with the operating system and workstation;
- operating system combined with workstation;
- integrated circuit smart cards;
- local computational network, including all the terminals, servers, network equipment and software;
- database application except remote client software, usually associated with the application database.



Picture 1. The concepts used in the valuation and their interconnection [7].

Security connected to the protection of assets. Assets are entities that represent value to anyone. Examples of assets include [7]:

- the contents of the file or server;
- software and hardware;
- the availability of the e-commerce process;
- access to limited access.

Become clear that identifying the vulnerability of systems or other objects and their evaluation, experts make conclusion what security tools to use, what methods of information security is the most reliable.

Analyze cybersecurity energy systems. The problem of cybersecurity energy systems is compounded by the fact that more than 75% of energy equipment is of foreign origin (not counting 100% computer and software) [8, 9]. The modern condition in automated control systems of technological processes (ASM TP) in the energy sector is characterized by the following numbers (the company Positive Technologies) [9]:

- every fifth vulnerability is eliminated for longer than a month.
- 50% of the vulnerabilities allow an attacker to execute code.
- 35% of vulnerabilities have exploits (special program for cyber attacks using the vulnerability).
- over 40% of Internet-accessible systems can hack hackers-lovers.
- a third of the Internet-accessible systems are in the United States.
- a quarter of vulnerabilities related to the absence of necessary security updates.
- Vulnerable 54% of Internet-accessible systems in Europe and 39% in North America.

There are several levels of technology in integrated networks [4]:

- level of generation transmission
- level of distribution
- level of consumption;
- level of management;
- information and communication level;
- physical level

Each of the above levels needed being continuously monitored to determine the good condition of the system, rapid response and reporting.

And for the smooth functioning of the infrastructure necessary to ensure information security on all levels of the network.

Information security today is the main area of concern in the world and its provision has considered being a priority. The energy sphere of the country is developing rapidly, as well as throughout the world, our main task is to build intelligent network by integrating alternative sources of energy in general electrical network for the prevention energy and economic losses with the absolute managing all of the power grid. And in the achievements of these goals and simultaneously, it is necessary to ensure the development of information security infrastructure based on international standards and, if necessary, develop national standards in security the energy sector.

References

1. Постановление Президента Республики Узбекистан, об ускоренных мерах по повышению энергоэффективности отраслей экономики и социальной сферы, внедрению энергосберегающих технологий и развитию возобновляемых источников энергии. № ПП-4422, г. Ташкент. 22 августа 2019 г.

2. Давронов Ш. Р., Иззатиллаев Ж.О. Основные аспекты управления электрической сетью с интегрированными солнечными электростанциями. Республиканская научно-практическая конференция 18-19 май 2018 год, Карши, -С. 97-101.

3. Smart Power Grids – Talking about a Revolution [Электронный ресурс] / IEEE Emerging Technology Portal, 2009.

4. Беляев А.Н., Ивановский Р.И., Карпов Ю.Г., Сотников К.А. СМАРТ ГРИД. Разработка приложений. Научно-технические ведомости СПбГПУ 6–1 2011НЕТЛ, Тхе НЕТЛ Модерн Грид Инитиативе Поуеринг оур 21ст-Сентури экономй: МОДЕРН ГРИД БЕНЕФИТС. Департмент оф энергй, 2007

5. ИСО/ИЕС 27001 Информационные технологии. Методы защиты. Системы менеджмента информационной безопасности. Требования.

6. ISO/IEC 15408-1 – Information technology. Security techniques. Evaluation criteria for IT security. Part 1. Introduction and general model.

7. Massel A., Massel L. The current state of cyber security in Russia's energy systems and the proposed activities for situation improving, Proceedings of the International Conference on Problems of Critical Infrastructures, 6th International Conference on Liberalization and Modernization of Power Systems. Edited by Z.A. Styczynski and N.I. Voropai. Saint Petersburg, 2015, pp. 183-189.

8. Massel A., Massel L. The current state of cyber security in Russia's energy systems and the proposed activities for situation improving, Proceedings of the International Conference on Problems of Critical Infrastructures, 6th International Conference on Liberalization and Modernization of Power Systems. Edited by Z.A. Styczynski and N.I. Voropai. Saint Petersburg, 2015, pp. 183-189.

9. Массел Л.В., Воропай Н.И., Сендеров С.М., Массел А.Г., Киберопасностъ как одна из стратегических угроз энергетической безопасности России. Вопросы кибербезопасности №4 (17) 2016.

REZYUME

Aqlli tarmoqlar tushunchasi nisbatan yaqinda paydo bo'ldi va butun dunyoni qamrab olishga muvaffaq bo'ldi. Aynan shu yo'nalishda rivojlanayotgan mamlakatlarning energetik infratuzilmasi yangilanishga muhtoj edi. Ammo ushbu miqyosdagi intellektual elektr tar-

moqlarining integratsiyasi, albatta, axborot xavfsizligini yuqori darajada ta'minlashni talab qiladi. Ushbu maqolada integratsiyalangan tarmoqni joriy qilish va xavfsizligini ta'minlash uchun xalqaro axborot xavfsizligi standartlari ko'rib chiqiladi.

РЕЗЮМЕ

Понятие интеллектуальных сетей появилось относительно недавно и успело охватить весь мир. Так как именно обновление в этом направлении нуждалось в энергетической инфраструктуре развивающихся стран. Но интеграция интеллектуальных электрических сетей такого масштаба обязательно требует обеспечения информационной безопасности на высоком уровне. В работе рассматриваются международные стандарты по информационной безопасности для внедрения и обеспечения безопасности интегрированной сети.

SUMMARY

The concept of intelligent networks appeared relatively recently and managed to cover the whole world. The energy infrastructure of developing countries needed to be updated in this direction. But the integration of intelligent electrical networks of this magnitude necessarily requires ensuring information security at a high level. In this work we discuss international standards in information security for the implementation and security of an integrated network.

КОМПЬЮТЕР ГРАФИКАСИ ТАЛАБАЛАРНИНГ ФАЗОВИЙ ТАСАВВУРИ РИВОЖЛАНИШИНИНГ ОМИЛИ СИФАТИДА

Ш.Д.Дилшодбеков – *докторант*

Низомий номидаги Тошкент давлат педагогика университети

Таянч сўзлар: фазо, тасаввур, фазовий тасаввур, фазовий визуаллаштириш, CAD дастурлари.

Ключевые слова: пространство, воображение, пространственное воображение, пространственная визуализация, CAD программы.

Key words: space, imagination, spatial imagination, spatial visualization, CAD programs.

Бугунги кунда, компьютер технологиялари кўпгина қийин бўлган ҳисоблаш жараёнларини ўз зиммасига олди. Масалан, автомат проекциялаш ва 3D моделлаштириш. Аммо бу жараёнларнинг автоматлашуви фазовий тасаввурни ривожлантириш ёки чизма бажаришда муҳандислик графикасида қўлланиладиган усуллардан фойдаланиш шарт эмас, деган фикрга олиб келмайди. Компьютер технологиялари қанчалик кучли бўлмасин, одамларсиз у ўзининг моҳиятини йўқотади [1].

Фазо арабча сўз бўлиб, «очиқ кенг майдон; коинот; ҳамма томонга чексиз йўналган бўшлиқ; осмон» маъносини англатади.

Тасаввур – кишининг нарса, ходиса ва шу кабилар ҳақидаги тажрибага асосланган билим-тушунчаси.

Фазовий тасаввур – предметнинг фазовий шаклини идрок қилмоғи-кўрмоғи, эшитмоғи ва шу жараённи кўз олдига келтиришни ёки тасаввур қилиш қобилияти [2].

Фазовий тасаввур қобилияти ва фазовий тасаввур кўникмаси терминлари бир-бирига ўхшаш маъноларни берсада, улар орасида фарқ борлигини таълим психологияси таъкидлайди. Фазовий тасаввур қобилияти ҳаёлда бирон-бир буюмни визуаллаштиришнинг туғма кўриниши бўлса, фазовий тасаввур кўникмаси эса ўқиш натижасида шакллантирилган ёки орттирилган қобилият [3].

Талабаларнинг фазовий тасаввурини ривожлантириш масалалари И.Раҳмонов, Э.Рўзиев, Д.Ф.Қўчқорова ва б.қ. лар томонидан тадқиқ этилган. Лекин, талабалар фазовий тасаввурларининг компонентлари ҳақида маълумотлар етарлича эмас. Қолаверса, талабаларнинг фазовий тасаввурларини бошқариш ва уларда бу қобилиятни бир ҳилда ривожланиши масаласи чуқур ёритилмаган.

Гее М.Г. [4] ва Майер П.Х. [5] лар фазовий тасаввурнинг бешта компоненти бор эканлигини такъдлаб ўтишган. Улар: фазовий қабул қилиш, фазовий визуализация, менталь айлантириш, фазовий муносабат ва фазовий ориентация.

Тартре Л.А. юқорида келтирилган фазовий тасаввурнинг бешта компонентида ўхшашликлар бор деб ҳисоблаб, уларни иккита фазовий визуализация ва фазовий ориентация каби категорияларга ажратган [6].

Фазовий визуализация бирон-бир буюмни ҳаёлан айлантириш, унга ўзгартириш киритиш қобилияти бўлса, фазовий ориентация эса, жисмларнинг жойлашувини тушунишдир [4].

Фазовий визуализацияда инсон онгида жисмни жойлашувини ўзгартириш назарда тутилса, фазовий ориентацияда эса, кўриш нуқтасини ўзгартириш назарда тутилади. Яъни, фазовий ориентацияда жисм жойида туради, кўриш нуқтаси ёки одам жисм атрофида айланади [7].

Ёш ҳусусиятларини инобатга олган ҳолда, оламни англаш ва фазовий қабул қилиш тўрт босқичга ажратилган. Биринчиси, сенсомотор босқич - туғилгандан 2 ёш бўлгунга қадар вақтни ўз ичига олади. Иккинчиси, интуитив босқич – 2 ёшдан 7 ёшгача. Учинчи босқич 7 ёшдан 12 ёшгача бўлган вақтни ўз ичига олади. Охирги босқич формаль операцион бўлиб, 13 ёшдан бошланади ва катта ёшгача давом этади (ҳаммада ҳар хил) [8].

Фазовий тасаввурга таъсир этувчи омилларга ёш, тажриба ва жинс кабиларни киритиш мумкин [4]. Муҳандислик таълимида гендер масаласи ёш ва тажрибага нисбатан муҳим аҳамият касб этади. Ёш ва тажриба фазовий тасаввурга гендер масаласи каби кучли таъсир кўрсатмайди [9].

Фазовий тасаввур бўйича олиб борилган тадқиқотларнинг тарихини Стронг С. ва Смит Р.лар 4 босқичга бўлишган.

Биринчи босқич 1901–1938 йилларни ўз ичига олган ва психологлар томонидан фазовий тасаввур ривожланишига таъсир этувчи ягона факторни аниқлаш билан характерланади. Иккинчи босқич 1938-1961 йилларни ўз ичига олади. Бу даврда бир нечта факторни аниқлаш бўйича иш олиб борилган. Учинчи босқич 1961-1982 йилларда. Фазовий тасаввур ривожланишига таъсир этувчи факторларни янада кўпайиши кузатилади. Масалан, ёш, жинс ва тажриба. Муҳандислик компьютер дастурларида 2D-3D тушунчалари пайдо бўлади. 1970 йиллардан бошлаб CAD тизимлари самарали ва инкор этиб бўлмас инструментга айланди. Бу даврда CAD тизимлари фақат чизмани электрон бажариш имконини берган. Тўртинчи босқич ҳозирги кунгача бўлган даврни ўз ичига олади. Бу даврда, компьютер технологияларининг фазовий тасаввурнинг ривожланишига ижобий таъсири кузатилмоқда. 2D ва 3D CAD тизимлари муҳандислик графикаси таълимигадаги иштироки таъминланди [7].

Бизнинг фикримизча, талабаларнинг фазовий тасаввурини ривожлантиришда CAD тизимларидан фойдаланиш ижобий натижа беради. Қолаверса, талабаларнинг фазовий тасаввурини ривожланганлик даражасини аниқлаш ва гурухдаги барча талабаларда фазовий тасаввурнинг бир хилда ривожланишини назорат қилиш учун энг қулай воситадир.

Фазовий тасаввурни ривожлантириш ўқиш даврининг биринчи босқичидан бошланиши зарур деб биламиз. Бу вазифани муҳандислик графикаси фанларидан «Чизма геометрия» фани зиммасига