O‘ZBEKISTON RESPUBLIKASI OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

MIRZO ULUG‘BEK NOMIDAGI O‘ZBEKISTON MILLIY UNIVERSITETINING JIZZAX FILIALI

ZAMONAVIY INNOVATSION TADQIQOTLARNING DOLZARB MUAMMOLARI VA RIVOJLANISH TENDENSIYALARI: YECHIMLAR VA ISTIQBOLLAR

mavzusidagi Respublika ilmiy-texnik anjuman materiallari to‘plami

(2024-yil 17-18-may)

(1-qism)

JIZZAX-2024

“Zamonaviy innovatsion tadqiqotlarning dolzarb muammolari va rivojlanish tendensiyalari: yechimlar va istiqbollar” mavzusidagi Respublika ilmiy-texnik anjuman materiallari to‘plami – Jizzax: O‘zMU Jizzax filiali, 2024-yil 17-18-may. 410-bet.

Respublika miqyosidagi ilmiy-texnik anjuman materiallarida zamonaviy innovatsion tadqiqotlarning dolzarb muammolari va rivojlanish tendensiyalari sohasidagi innovatsion tadqiqotlar aks etgan.

Globallashuv sharoitida davlatimizni yanada barqaror va jadal sur’atlar bilan rivojlantirish bo‘yicha amalga oshirilayotgan islohotlar samarasini yaxshilash sohasidagi ilmiy-tadqiqot ishlariga alohida e’tibor qaratilgan. Zero iqtisodiyotning, ijtimoiy sohalarni qamrab olgan modernizatsiya jarayonlari, hayotning barcha sohalarini liberallashtirishni talab qilmoqda.

Ushbu ilmiy ma’ruza tezislari to‘plamida mamlakatimiz va xorijlik turli yo‘nalishlarda faoliyat olib borayotgan mutaxassislar, olimlar, professor-o‘qituvchilar, ilmiy tadqiqot institutlari va markazlarining ilmiy xodimlari, tadqiqotchilari, magistr va talabalarning ilmiy-tadqiqot ishlari natijalari mujassamlashgan.

Mas’ul muharrirlar: DSc.prof. Turakulov O.X., PhD. O‘ralov A.I.

Tahrir hay’ati a’zolari: p.f.d.(DSc), prof. Turakulov O.X., b.f.f.d. (PhD) O‘ralov A.I., t.f.f.d.(PhD), dotsent Abdumalikov A.A., t.f.n., dots. Baboyev A.M., t.f.f.d.(PhD), dots. Abduraxmanov R.A., p.f.f.d.(PhD) Eshankulov B.S., p.f.n., dots. Alimov N.N., p.f.f.d.(PhD), dotsent Alibayev S.X., p.f.f.d. (PhD) Halimov O‘.H., p.f.f.d.(PhD), dotsent Karshiyev A.A., f.f.f.d.(PhD), dotsent Sindorov L.K., t.f.f.d.(PhD), dotsent Nasirov B.U., b.f.f.d. (PhD), dotsent Mustafaqulov M.A., f.f.f.d. (PhD) Alibekov D.A.., f-m.f.f.d. (PhD) Sharipov X.F., ps.f.f.d.(PhD) Norbekova B.Sh., i.f.n., dots. Tsoy M.P., Qayumov O.A., Jo‘rayev M.M.

Mazkur to‘plamga kiritilgan ma’ruza tezislarining mazmuni, undagi statistik ma’lumotlar va me’yoriy hujjatlarning to‘g‘riligi hamda tanqidiy fikr-mulohazalar, keltirilgan takliflarga mualliflarning o‘zlari mas’uldirlar.

РАЗРАБОТКА АЛГОРИТМ ОБНАРУЖЕНИЯ И ОБЕЗВРЕЖИВАНИЯ УГРОЗ НА ОСНОВЕ ТАБЛИЦ ФУНКЦИОНИРОВАНИЯ

[1,2,3]д.ф.-м.н., проф. Норматов Иброхимали Холмаматович,
Каримов Раджабмурод, Мирзахмедова Эъзоза
[1,2,3]Национальный университет Узбекистана имени Мирзо Улугбека
ihnormatov@Gmail.com

Аннотация. В статье дается анализ систем, предназначенных для сбора и автоматического анализа событий различных информаций с целью выявления угроз. Предлагается разработка таблицы функционирования и граф-схемы переходов угроз на основе использования сети Петри для визуального отображения любых действий в системе в реальном процессе, а также предлагается алгоритмическая система и вычислительные алгоритмы обнаружения и обезвреживания угроз при обеспечении защиты информации на основе таблиц функционирования (ТФ).

Ключевые слова: алгоритм, система, модель, агрегат, таблица функционирования, угрозы, риск, управления, информационная система, программа, обнаружение, обезвреживание.

Системный подход к информационной безопасности (ИБ) требует выделять ее субъекты, средства и объекты, принципы обеспечения, источники опасности, направленность опасных информационных потоков.

Эволюция информационных технологий связана с интеллектуальными системами, в которых присутствуют процессы зарождения, адаптации и развития. Принцип моделируемости позволяет предотвратить ошибки проектирования кибернетических систем, а принцип связности при разработке эффективной системы рассматривает объект защиты комплексно, объединяя объект защиты, внешнюю среду, средства защиты и угрозы злоумышленника и учитывая взаимосвязи: источник угрозы – уязвимость – действие – атака.

Построение системы защиты является обязательным условием для обеспечения безопасности КИ, хранимой и обрабатываемой в информационной системе. Требования к системе защиты информации формируются по результатам проведения обследования информационной системы и ориентированы на нейтрализацию уязвимостей системы. Одним из способов анализа защищенности системы производится на основе динамических ТФ информационной системы на базе сетей Петри [1]. С помощью алгоритмической модели на основе ТФ проводится обследование функционирования реализованной системы защиты, и выявляются ее недостатки.

Моделирование на основе ТФ осуществляется на событийном уровне. Определяются, какие действия происходят в системе, какие состояния предшествовали этим действиям и какие состояния примет система после выполнения действия. Выполнения событийной модели в таблице функционирования описывает поведение системы. Анализ результатов выполнения может сказать о том, в каких состояниях пребывала или не пребывала система, какие состояния в принципе не достижимы.

Таким образом, кроме вышеизложенного в таблице функционирования также вычисляются все возможные риски, угрожающие работоспособности информационной системы, а также риски для всех имеющих ценностей информаций в системе.

Одним из способов анализа защищенности системы является построение динамических ТФ ИС [2-6]. С помощью алгоритмической модели на основе ТФ проводится обследование функционирования реализованной системы защиты, и выявляются ее недостатки. Алгоритмические модели на основе ТФ [2,3] используются как математический аппарат для моделирования динамических дискретных систем, обеспечивающий комплексную защиту ИС от всех внешних и внутренних угроз по заданной логической последовательности. Алгоритмическая модель обеспечения комплексной защиты ИС состоит из несколько основных частей:

1. Общая структурная модель обеспечения безопасности ИС на основе таблицы функционирования;

2. Математическая модель идентификации угроз от внешних и внутренних источников;

3. Синтез и анализ построения таблицы функционирования после получения необходимых данных на этапе «СИНТЕЗ»;

4. Пути, способы, методы, модели и средства уничтожения обнаруженных угроз. Здесь можно получить информацию об уничтожении последовательности обнаруженных угроз в ТФ в виде графа;

5. Анализ возможных угроз на информационную систему, анализ рисков и анализ защищенности ИС.

Использование сети Петри для визуального отображения любых действий в системе в реальном процессе является самим оптимальным решением. Процесс функционирования сети Петри может быть наглядно представлен графом достижимых маркировок. Состояние сети однозначно определяется её маркировкой-распределением фишек по позициям. Вершинами графа являются допустимые маркировки сети Петри, дуги помечены символом срабатывающего перехода. Дуга строится для каждого активированного перехода. Построение прекращается, когда мы получаем маркировки, в которых не активирован ни один переход либо нет маркировки, содержащиеся в графе. Пример траектории в сети Петри задана на рис 1.

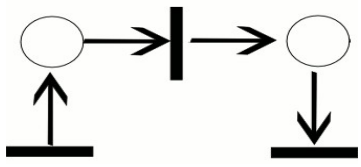


Рис.1. Пример траектории в сети Петри

Сети Петри используются для моделирования асинхронных систем, функционирующих как совокупность параллельных взаимодействующих процессов. Построение системы защиты является обязательным условием для обеспечения безопасности КИ, хранимой и обрабатываемой в информационной системе.

Развитие ИС обработки и хранения КИ диктует необходимость построения надёжной системы защиты КИ (СЗКИ).

Построение СЗКИ проводится в несколько этапов. Первым этапом является обследование ИС, в рамках которого анализируется технология обработки, хранения и защиты информации, формируется модель нарушителя и модель угроз безопасности КИ, а также составляются требования к СЗКИ. Требования к СЗКИ, в зависимости от вида КИ определяются согласно нормативно-законодательной базы Государства.

Один из главной особенности ТФ является идентификация угроз распределения его по критериям, характеристиками и оказывающим негативными действиями систему. В данном случае ранее не известные угрозы после сканирования сравниваются уже известными классами угроз. Если угроза является уникальным для неё в ТФ отделяется отдельное ячейка, а если таковым не является тогда данную угрозу добавляют наиболее подходящим классам угроз.

Моделирование на основе ТФ осуществляется на событийном уровне. Определяются, какие действия происходят в системе, какие состояния предшествовали этим действиям и какие состояния примет система после выполнения действия. Выполнения событийной модели в ТФ описывает поведение системы. Анализ результатов выполнения может сказать о том, в каких состояниях пребывала или не пребывала система, какие состояния в принципе не достижимы.

Если и функция, $F(t_i) = const$ то такая таблица функционирования называется статической (стационарной). Функция F(t), задающая изменения таблицы функционирования, называется функцией управления агрегатной системой или функцией планирования процессов в системе.

В каждый интервал времени t_i описание ТФ представляется в виде маркированной сети Петри: $M= \{P, D, I, O, \mu\}$, где P, D, I, O - соответственно, множества состояний, переходов, входных и выходных состояний; μ-функция, отображающая множество состояний в множестве натуральных чисел .

Каждая маркировка μ может быть представлена как вектор $\mu = (\mu_1, \mu_2, ..., \mu_n)$, здесь . Вектор μопределяет для каждой позицииP_i сети количество фишек, т.е. для выполняется $\mu(pi)=$

Таким образом, за неделимый элемент динамических дискретных систем принято рабочее место (РМ), соответствующее α_i определённому решению предотвращения угроз. Обозначим его через α_i, а множество РМ -через А. Каждое α_i может быть представлено в виде работников, работника плюс машины

или машины. Каждое α_i имеет входы x и выходы y, внутреннее z состояние. На входы передаются сигналы или материалы в виде продуктов, веществ и т.д. Некоторые входные воздействия сигналов могут быть управляющими (g). В качестве машин применяются станки и вычислительные машины. Машины выступают в качестве орудия труда, а информация, материалы - в качестве предметов труда.

В процессе функционирования системы структура сети со временем может меняться: старые дуги и вершины аннулируются, а новые добавляются. Такие сети назовём ситуационными или RC - сетями. При решении определённого класса задач в течение времени (t_1, t_2) на каждом α выполняется одна из приписанных ему операций. Поэтому построение самой сети и определение приписанной операции является основной задачей системных исследований. В определённый промежуток времени сеть можно изобразить в виде ориентированного графа неизменной структуры (рис.1).

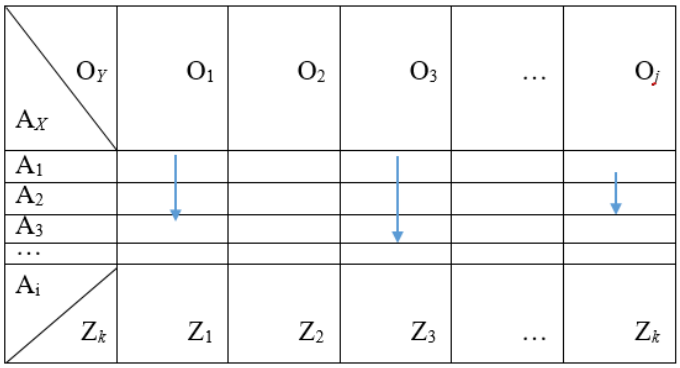


Рис. 1. Таблица функционирования

Если машины, которые должные обрабатывать и уничтожить угрозы не смогут выполнить свою работу данная задача передаётся другой машины, стоящей ниже. В конечном итоге угроза должна быть уничтожена, в ином случае система оповестит о не уничтоженным угрозой в системе (Рис. 2.).

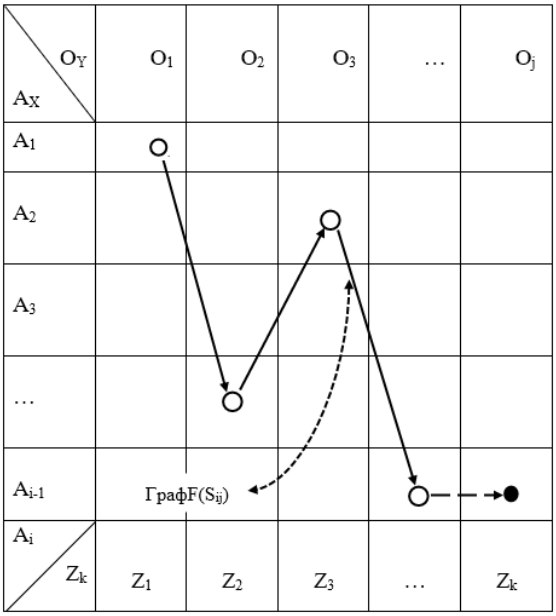


Рис. 2. Графы переходов угроз

В первом примере считается, что угроза ранее была рассмотрена и поэтому ее источник сразу блокируется и удаляется (рис.3). Угроза предотвращается, не причинив вреда системе.

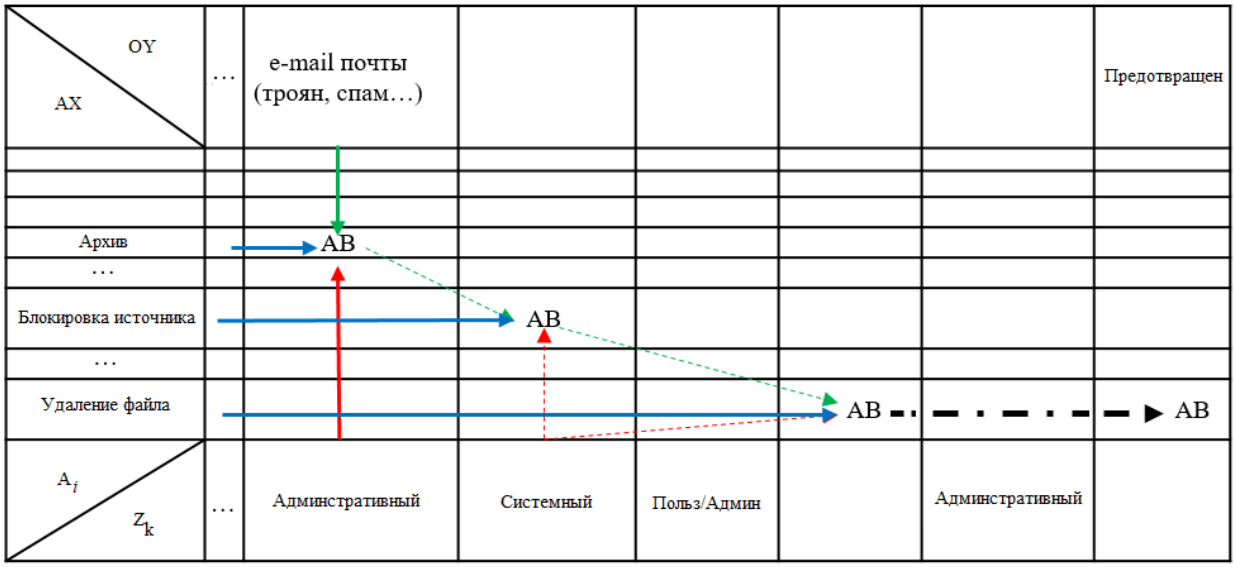


Рис.3. Пример таблицы функционирования

Таким образом в работе предложена построение алгоритмической модели СКЗИ для исследования сложных ИС на основе ТФ. С точки зрения ИБ алгоритмические модели на основе ТФ используются как математический аппарат для моделирования динамических дискретных систем.

Расчёты по переходам осуществляются следующим способом.

В ТФ по вертикали имеются 127 средств защиты от угроз (антиугрозы). Если проникающая угроза является комбинированной, тогда она проверяется в каждом ячейке, т.е. 127 раз угроза обрабатывается системой.

Для вычисления более эффективного переходя для уничтожения угроз имеем формулу $P = \sum_{i=1}^{\infty} U_i$, где U – Угроза P – переходы по ТФ.

Пусть A – антиугрозы, *K* – класс угроз. Когда у U=1, тогда P_{max}=127. Когда U=2, тогда P_{max}=254. Значить .

Если определены класс угроз и по классу пути уничтожения угрозы тоже ясны тогда формула будет следующим:

Здесь, если в угрозах один из классов не определяется, то она равняется к 0.

Поскольку угрозы проникают разнообразными способами, для вычисления эффективного пути уничтожения угроз невозможно использовать одну или несколько из них. Необходимо использование всех антиугроз. Значить $P = \sum_{i=1}^{9} P_{\max_i}$.

Если проникающая угроза является не комбинированной тогда максимум обрабатывая ячейка будет исчисляется по вертикали считывая строки, а минимальная будет равен на одного.

Таким образом, $\text{ТФ} = \{X, Y, A, O, \Theta, T, U, S, F, P\}$ – алгоритмическая модель АСУ обеспечения безопасности ИС, а также предотвращения любого вида угроз к ИС и информационным ресурсам (ИР), где

Y – множество возможных угроз $Y\{O_j\}$;

X – множество решений предотвращения угроз $X\{A_i\}$;

A – определённое решение предотвращения угроз;

O – определённое действие угроз;

Θ – координаты между «A_i» и «O_j»;

T – время (для предотвращения и успешной реализации угрозы);

U – внешнее воздействие (на $\Theta_{ij}\{A_i : O_j\}$);

S – множество переходов (переход из одной Θ_{ij} на другую $\Theta_{i+n, j+m}$);

$F(t)$ – функция изменения таблицы функционирования во времени;

P – множество вычислительных и логических операций ввода, вывода и управления;

Z – множество привилегий.

На основе сетей Петри мы создадим блок схему СКЗИ (рис.4) и гибридного варианта сетей Петри в обеспечении ИБ. В блок схеме основным шагам является обнаружение угроз «Y», после идентификации угрозы «O_j» она проверяется общим архивом(П+И) просмотренных угроз. Если угрозы такова вида были рассмотрены ранее она сразу нормализируется соответственными действиями «$P_{ij}F$». Если угроза рассматривается первые тогда она анализируется и вычисляется «Y, P_{ij}, U_{ij}, T_{ij}, O_j, A_i». После анализа источника Y+Z и анализ привилегии Z_k угрозы не обнаружатся тогда она пересматриваются $Y+Z_k$. После этого добавляются в архив пропущенных угроз (П). Если при анализе и вычислении угроза обнаружатся, то тогда действия будет идти по блок схеме №1, Продолжение. Здесь после всех шагов угроза добавляются в архив для быстрого обнаружения и идентификации угроз.

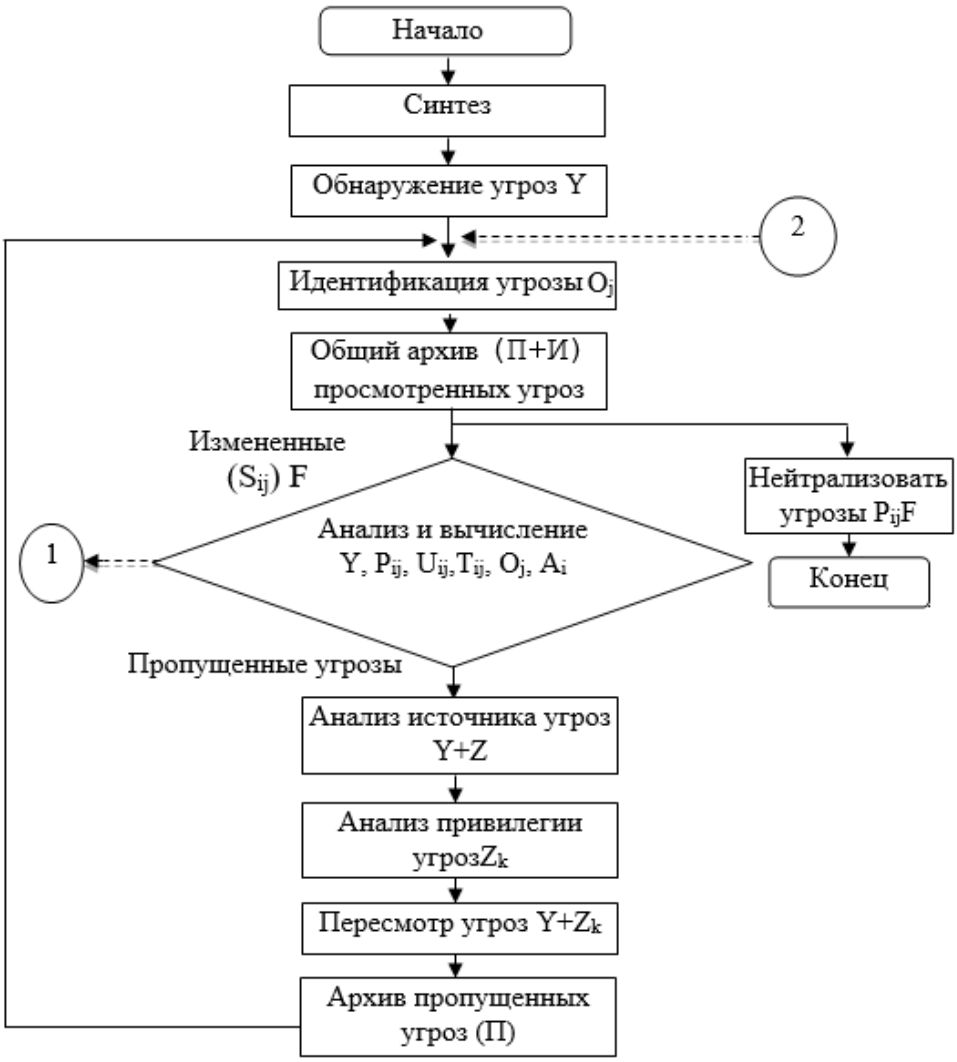


Рис.4. Блок схема СКЗИ системами действий сетей Петри

Таким образом, в работе предложено построение алгоритмической модели СКЗИ для исследования сложных ИС на основе ТФ. С точки зрения ИБ алгоритмические модели на основе ТФ используются как математический аппарат для моделирования динамических дискретных систем.

Список использованной литературы:

1. Дж.Питерсон Теория сетей Петри и моделирование систем//- М.: Мир, 1984.

2. Кабулов В.К., Кабулов А.В., Норматов И.Х. Алгоритмизация в теории управляющих систем//Монография: Ташкент-2017, Изд. “Навруз” С.176.

3. Кабулов В.К., Кабулов А.В., Норматов И.Х. ЛОГИЧЕСКИЕ МЕТОДЫ АЛГОРИТМИЗАЦИИ В ТЕОРИИ УПРАВЛЯЮЩИХ СИСТЕМ. Монография: Германия.2018, Изд. “Ламберт” с.191.

4. Кабулов А.В., Варисов А. Algorithmic information security models on the basis of operation tables// The 4th International conference on big data applications and services (BIGDAS 2017) proceeding August 15-18,2017, Tashkent, Uzbekistan. National University of Uzbekistan and Korea Big Data Service Society.

5. Кабулов А.В., Варисов А. Алгоритмические модели информационной безопасности на основе таблиц функционирования// Международный журнал «Наука и мир». №6,2017, том1 с. 28-33. Волгоград.

6. A.V. Kabulov, I.X. Normatov, I.I.Kalandarov, A.A.Karimov. Algorithmic Method of Organization of Specialized Workshops. International Journal of Advanced Research in Science, Engineering and Technology Vol. 5, Issue 4, April 2018, c.5670-5675, ISSN: 2350-0328.

INFOKOMMUNIKATSIYA OBYEKTLARINING ENERGIYA TARMOG‘INI KRIPTOGRAFIK XAVFSIZLIGINI TA’MINLASH

p.f.f.d, dots. Mingboev Ulug‘bek Xujayevich
O‘zbekiston Milliy universiteti Jizzax filiali
Abdurasulov Alijon Abdurasul o‘g‘li
O‘zbekiston Milliy universiteti Jizzax filiali magistranti
ulugbekmingboyev@gmail.com

Annotatsiya. Infokommunikatsiya obyektlaridagi aloqa va axborot uzatishni ta’minlashda muhim rol o‘ynaydi. Biroq, texnologiyalarning rivojlanishi va uzatiladigan ma’lumotlar hajmining ko‘payishi bilan infokommunikatsiya obyektlarning xavfsizligini ta’minlash zarurati tug‘iladi.Axborotni ruxsatsiz kirish va hujumlardan himoya qilish uchun asos bo‘lgan kriptografik energiya tizimining xavfsizligini ta’minlashga ham alohida e’tibor qaratilmoqda.

Kalit so‘zlar. Axborot xavfsizligi, infokommunikatsiya obyektlari, axborot hujumlari, kriptografiya, shifrlash, axborot ta’minoti,kiberxavfsizlik.

Respublikamizda raqamli iqtisod va axborot kommunikatsiya sohasini takomillashtirish asosida infokommunikatsiya obyektlarining elektr energiya ta’minoti ko‘rsatkichlarini monitoring tizimini takomillashtirishga qaratilgan keng qamrovli chora-tadbirlar amalga oshirilmoqda. 2022-2026 yillarga mo‘ljallangan yangi O‘zbekistonning taraqqiyot strategiyasida, jumladan «Yashil iqtisodiyot texnologiyalarini barcha sohalarga faol joriy etish orqali 2026 yilga qadar iqtisodiyotning energiya samaradorligini 20%ga oshirish va havoga chiqariladigan zararli gazlar hajmini 20%ga qisqartirish choralarini ko‘rish» vazifalari belgilangan. Mazkur vazifalarni bajarishda shu jumladan energiya manbalarini monitoring jarayonlarini modellashtirish, algoritmlash va ularni amaliy faoliyatga qo‘llash muhim vazifalardan biri hisoblanadi.

Hozirgi davrga kelib hayotimizni axborot texnologiyasi, kompyutersiz tasavvur qilish mumkin emas.“Axborot” tushunchasi sotib olish, sotish, biror boshqa tovarga almashtirish mumkin bo‘lgan maxsus tovar belgisi sifatida tez-tez ishlatilmoqda. Zamonaviy infokommunikatsiya obyektlari axborotni himoya qilish uchun kriptografik usullardan tobora ko‘proq foydalanmoqda.Biroq, kriptografik energiya tizimining xavfsizligi ma’lumotlarning yaxlitligi va maxfiyligini ta’minlashda ham muhim rol o‘ynashini unutmaslik kerak. Kriptografik energiya tizimining xavfsizligini