УДК 621.039:004.056:004.7

Погосов А. Ю.[1], Деревянко О. В.[2]

[1]Д-р техн. наук, профессор, профессор кафедры атомных электрических станций Института энергетики и компьютерно-интегрированных систем управления Одесского национального политехнического университета, Одесса, Украина

[2]Канд. техн. наук, старший преподаватель кафедры атомных электрических станций Института энергетики и компьютерно-интегрированных систем управления Одесского национального политехнического университета, Одесса, Украина

МОДЕЛИ ПРИКЛАДНОЙ ИНФОРМАТИКИ УЧЕТА КИНЕТИКИ КИБЕРНЕТИЧЕСКИХ УГРОЗ В СИСТЕМЕ ФИЗИЧЕСКОЙ ЗАЩИТЫ АЭС

Актуальность. Рассмотрены актуальные подходы к превентивным оценкам и математическому моделированию процессов кибернетических атак и поступления внешних техногенных информационных угроз, которые могут быть направленны на систему физической защиты энергоблоков современных атомных электрических станций.

Цель работы – адаптация известных математических моделей кинетики кибератак для использования в системе информационной безопасности и физической защиты АЭС к современным и прогнозируемым условиям.

Метод. Предложен метод адаптации модельных зависимостей, отражающих кинетику кибератак условиям эксплуатации защищаемых объектов атомной энергетики. Для совершенствования модельных зависимостей предложено модифицировать классическую функцию Ферхюльста и при математическом моделировании кибернетических атак на объекты атомной энергетики использовать соответствующую трансформацию логистической кривой, которая имеет характерную особенность в виде четко выраженного максимума.

Результаты. Предсказано, что модельная зависимость потока внешних по отношению к АЭС кибернетических угроз может характеризоваться чередованием минимумов и максимумов, что указывает на возможность колебательного характера развивающегося процесса. Также выдвинута и обоснована гипотеза о том, что система физической, и в частности, кибернетической, защиты АЭС может характеризоваться временным запаздыванием, что с учетом возможного колебательного характера процесса поступления информационных угроз создает предпосылки для развития колебательной неустойчивости. Результаты, полученные в ходе исследований, носят прикладной характер, могут быть использованы для проведения широкомасштабных экспериментов и прогнозирования параметров направленных на АЭС возможных кибернетических угроз с целью их упреждения и превентивного обеспечения информационной безопасности современных ядерных энерготехнологий.

Выводы. Рекомендуемые к использованию модельные зависимости впервые адаптированы к условиям эксплуатации объектов атомной энергетики, учитывают факторы противодействия угрозам и обстоятельства, связанные со специфическим временным запаздыванием.

Впервые показано, что существует возможность как экстремального, так и колебательного характера зависимости интенсивности кибернетических атак, направленных на систему программно-технических средств информационной безопасности АЭС. Новый подход позволяет предположить реальность развития неустойчивого колебательного процесса в системе «нападение – защита» и дает возможность превентивной оценки соответствующих запасов устойчивости.

Практическая значимость состоит в том, что полученные результаты позволяют реалистично оценивать время наступления ожидаемых изменений текущей зависимости кибератак и использовать эти знания для организационно-технической подготовки средств защиты и заблаговременного упреждения IT-угроз.

Ключевые слова: прикладная информатика, информационная безопасность, физическая защита АЭС, математическое моделирование кибернетических атак на объекты атомной энергетики.

НОМЕНКЛАТУРА

IT – Information Technology (информационные технологии);

АЭС – Атомная электрическая станция;

K_i – уровень насыщения интенсивности кибератак;

r_i^m – параметр крутизны начального возрастания интенсивности кибератак;

t_0 – начальный момент времени;

t – текущее время;

$x_i(t)$ – интенсивность кибератак;

x_i^0 – начальное значение интенсивности кибератак;

γ – коэффициент пропорциональности, определяемый путем статистической верификации модели.

ВВЕДЕНИЕ

В соответствии с международными рекомендациями [1] и требованиями законодательных актов Украины [2, 3 и др.] система физической защиты атомных электростанций (АЭС) предусматривает инженерно-технические мероприятия, которые проводятся с целью создания условий, направленных на минимизацию возможности совершения диверсий, краж или каких-либо других неправомерных изъятий радиоактивных материалов, снижения вероятности осуществления иных противоправных действий в отношении объектов атомной энергетики. Ранее считалось, что инженерно-технические сооружения, препятствующие проникновению посторонних лиц на территорию АЭС, являются надежным средством защиты этих объектов. Однако, с расширением применения информационных технологий [4] на объектах атомной энергетики, стало понятно, что к числу угроз для АЭС объективно могут быть отнесены и попытки кибернетических атак [5, 6] – компьютерно-интегрированных покушений на информационную безопасность систем, обеспечивающих нормальные условия

DOI 10.15588/1607-3274-2017-2-6

работы штатного оборудования и выполняющих функции управления и защиты.

Исходя из этого, в соответствии с Законом [2], к первоочередным требованиям, предъявляемым к системе физической защиты АЭС, теперь относится, в частности, создание условий для защиты информации с ограниченным доступом [7, 8], поскольку информационная безопасность таких объектов является необходимым условием обеспечения их физической защиты. Такого рода защита сигнальной (компьютерно-интегрированной) информации, как один из аспектов прикладной информатики, становится все более актуальной для атомной энергетики.

Математические модели, используемые в экспертных системах обеспечения информационной безопасности и физической защиты АЭС относятся к важным информационным ресурсам упреждения нежелательных IT-воздействий (кибернетических атак) и одним из факторов эффективности, надежности и безаварийности атомных электростанций. Анализ кинетики IT-угроз, направленных на АЭС, выявляет необходимость использования постоянно совершенствуемых математических моделей для адекватного обновления соответствующих экспертных систем компьютеризированной защиты атомных электростанций.

Объектом данного исследования является процесс отражения кибернетических атак на АЭС. Предметом исследования являются математические подходы и модели, описывающие кинетику кибератак на объекты атомной энергетики.

Целью работы является адаптация известных математических моделей кинетики кибератак для использования в системе информационной безопасности и физической защиты АЭС к современным и прогнозируемым условиям.

1 ПОСТАНОВКА ЗАДАЧИ

Для достижения цели в работе ставится и решается следующая двуединая задача: во-первых, – проанализировать возможность повышения адекватности моделирования кинетики направленных на АЭС выявленных и (или) блокированных внешних IT-угроз, во-вторых – определить пути совершенствования базовых математических моделей для оценки информационной безопасности АЭС.

Формальная постановка задачи заключается в следующем. Требуется проведение анализа существующих математических зависимостей, используемых в теории и практике аналитического моделирования сигнальных потоков, направленных на системы информационной безопасности охраняемых объектов для описания интенсивности $x_i(t)$ следования событий, каждое из которых в общем случае представляет собой некоторый акт направленного действия, имеющего нежелательный характер или нежелательные последствия и поэтому предусматривающий технически организованное противодействие или упреждение со стороны системы безопасности. Анализ должен выявить недостатки используемых аналитических зависимостей, не позволяющие адекватно оценивать поток информационно-технологических угроз для таких специфических объектов как атомные электростанции. По результатам анализа должен быть предложен подход к усовершенствованному аналитическому моделированию и предложена приемлемая математическая зависимость для описания интенсивности кибератак на АЭС, использование которой при моделировании нежелательных актов воздействия в рамках сигнально-информационного процесса позволит адекватно учитывать особенности информационных угроз для объектов атомной энергетики. При постановке задачи как исходное положение принимается, что информация – это какие-либо сведения и (или) данные, которые могут быть сохранены на материальных носителях (в том числе в форме сигналов) либо тем или иным образом отображены в электронном (компьютерно-адаптированном) виде. При решении поставленной задачи необходимо исходить из того, что под доступом к информации понимается возможность получения, обработки и преобразования информации, ее блокирование и (или) нарушение ее целостности. Соответственно, как условие должно быть принято положение, что ограничение доступа к информации может достигаться путем пресечения или предотвращения несанкционированных операций с компьютерными данными, если это имеет место или даже если существует риск (потенциальная опасность) проведения таких кибернетических операций.

В качестве результата исследования должны быть найдены новые возможности дальнейшего усовершенствования известных базовых математических моделей кинетики отражаемых угроз и предложены варианты адаптации известных в области прикладной информатики подходов к оценке информационной безопасности объектов атомной энергетики.

2 ОБЗОР ЛИТЕРАТУРЫ

Обзор опубликованных источников информации, на которые опираются наши исследования, показывает, что моделирование изменений во времени количества кибернетических инцидентов при рассмотрении классических задач информационной безопасности существенным образом зависит от специфики объекта, информационное пространство которого окружается системой защиты [1–9]. Однако, в большинстве случав, в области прикладной информатики для моделирования кинетики компьютерных угроз типа «программных вирусов» (во многом подобной кинетике размножения биологических вирусов, ферментативной кинетике и фармакокинетике), до недавнего времени – по крайней мере, к началу XXI века – апробированной и приемлемой являлась неспецифическая математическая модель, описывающая процесс изменения *x(t)* на основе аналитической зависимости Ферхюльста [7]:

$$x_i(t) = \frac{K_i}{1 + \frac{K_i - x_i^0}{x_i^0} e^{-r_i^m (t - t_0)}}, \qquad (1)$$

которая, с учетом соответствующих характерных параметров, определяет форму логистической кривой, графически представленной на рис. 1. Такая зависимость свойственна процесам в системе с неразвитой системой

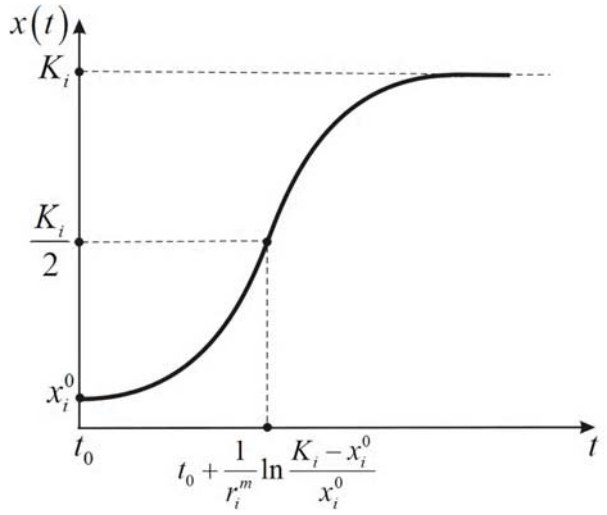

Рисунок 1 – Формообразующие параметры логистической кривой, отражающей кинетику организованных кибернетических атак в неспецифических задачах прикладной информатики для незащищенных объектов

защиты того или иного объекта от возможных внешних угроз и атак, в том числе – кибернетических атак, условия моделирования процесса поступления которых, начиная с первых основополагающих публикаций, подробно рассмотрены в [4].

Известно, что для полуограниченного интервала времени, ориентировочно относящегося к прошлому, на котором $x(t) \le K_i$ /2, участок графика, приведенный на рис. 1, в общих чертах отвечает экспоненциальной зависимости, характерной для процесса репликации биологических вирусов при отсутствии противодействующих факторов (противовирусных препаратов) или для процесса размножения компьютерных «вирусов» при отсутствии обезвреживающих программных средств (антивирусного программного обеспечения). Соответственно, начальный участок кривой, используемый при моделировании во многих задачах, практически совпадает с графической интерпретацией зависимости Мальтуса-Фибоначчи, ранее применявшейся для прогнозирования роста численности биологических популяций и предумышленных технических угроз незащищенным компьютерным программным ресурсам на начальном этапе развития кибернетики, как это было показано в [10].

Исходя из работ, опубликованных в последние годы, которые подробно рассмотрены и обобщены в [9], можно заключить, что интенсивность оперативных ограничений и противодействий, реализуемых программно-техническим (программно-компьютерным) комплексом системы физической безопасности АЭС, безусловно должна отвечать интенсивности организованных кибератак $x(t)$, а этого можно добиться лишь учитывая специфику защищаемого объекта и условия его функционирования. Исходя из этого, следует признать, что наиболее значимой в методическом плане, из числа работ, опубликованных в последние годы, представляется парадигма моделирования И. В. Кононович [9], трансцендентно устраняющая недостатки известных ранее подходов и методов благодаря продвижению прогрессивной идеологии пересмотра модели изменения $x(t)$ в новых специфических условиях формирования системы глобальной кибернетической безопасности.

Можно заключить, что анализ известных разработок в целом показывает, что известные подходы, апробированные в области прикладной информатики по отношению к широкому перечню объектов, ранее пригодные для решения широкого класса задач моделирования процессов возникновения инцидентов нарушения информационной безопасности объектов и успешно применявшиеся прежде в неспецифических задачах, нельзя признать удовлетворительными с учетом специфики эксплуатации АЭС в современных условиях. Исходя из этого положения, должны быть найдены возможности для математического моделирования процесса кибератак на АЭС, которые бы обеспечили учет как специфики защищаемых объектов атомной энергетики, так и изменение условий поступления информационных угроз по сравнению с предшествующим периодом.

3 МАТЕРИАЛЫ И МЕТОДЫ

Для преодоления недостатков известных подходов к моделированию в современных условиях процесса следования кибератак на объекты атомной энергетики используем информационные материалы, относящиеся к промежутку времени после реперной точки с ординатой K_i / 2, отмеченной на кривой, приведенной на рис. 2.

Для открытого интервала времени, ориентировочно обращенного в будущее, на котором $x(t) \ge K_i$ / 2, соответствующий сегмент графика отвечает зависимости, связанной с актуальным представлением о развитии процесса внешних кибернетических атак на физически (и кибернетически в том числе) защищаемые объекты. Исходя из имеющихся информационных материалов, методически важно обратить внимание на то, что рассматриваемый участок приведенного графика в общих чертах совпадает с графической интерпретацией уравнения ферментативной кинетики Михаэлиса-Ментен для биологических систем, обладающих способностью к внутренним противодействиям внешней активности [11].

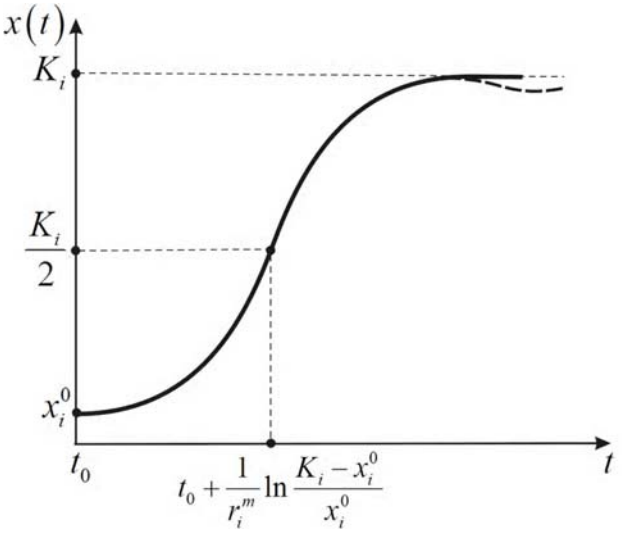

Рисунок 2 – Прогнозируемое изменение формы кривой, отражающей кинетику кибератак для случая объектов с ограниченным противодействием внешним угрозам (отклонение обозначено пунктирной линией)

Применение метода обобщения статистических данных и метода прямого сравнения позволяет обнаружить, что динамика поведения логистической функциональной зависимости (1), сочетано обладающей свойствами зависимости Мальтуса (Фибоначчи-Мальтуса) и зависимости Михаэлиса-Ментен, определяется тремя параметрами: x_i^0, K_i и r_i^m. Этим параметрам придается соответствующий физический смысл: первый из указанных параметров (x_i^0) определяет начальное значение численности кибератак на *i*-й (программный) объект защиты x_i при $t = t_0$, второй из указанных параметров указывает на уровень насыщения, к которому стремится $x_i(t)$, иначе – на граничную для данного объекта численность попыток воздействия, а параметр r_i^m задает крутизну начального возрастания рассматриваемой функциональной зависимости.

Формальный подход к обработке имеющегося информационного материала на основе дедуктивной логики позволяют также выяснить математический, а затем и технический смысл величин r_i^m и K_i (важный для понимания организации информационной безопасности конкретного технологического модуля защиты в пределах промплощадки АЭС). В этой связи необходимо отметить, что зависимость удельной скорости прироста информационных атак на защищаемый объект от плотности активно реализуемых программно-технических возможностей защиты объекта, которая имеет вид $r_i\left(x_i\right) = r_i^m - \gamma x_i$, является разложением в ряд Тейлора удельной скорости прироста атак на объект по степеням, зависящим от плотности активизации программно-технических возможностей конкретных защитных средств $x_{i,}$ которое представлено членами ряда с нулевой и первой степенью. Компонента этого разложения, которая отвечает нулевой степени ($r_{i_0} = r_i^m$), не зависит от x_i, а компонента, которая отвечает первой степени ($r_{i_1} = -\gamma x_i$) зависит от x_i, причем $r_{i_0} \to 0$ при $x_i \to 0$. Поэтому при малой начальной плотности x_{i_0} первичное возрастание возможностей защиты будет почти экспоненциальным с показателем степени r_i^m (как это полагалось в начальный период развития атомной энергетики), так что этот параметр является, по сути, оценкой защитного потенциала объекта, который оснащен средствами противодействия внешним угрозам. Параметр K_i, согласно формальной логике, характеризует емкость потенциала защищаемого объекта, и может быть выражен соответствующей предельной численностью отражаемых атак.

Как показывает проведенный анализ, адекватно (соответственно условиям текущего времени) выбирая величины x_i^0, K_i и r_i^m, можно более или менее удовлетворительно описывать кинетику изменений программно-аппаратных возможностей кибератак и защиты от них конкретного объекта. Однако описанную зависимость логистического характера следует рассматривать лишь как одну из возможных математических моделей кинетики в системе «злоумышленник – защитник», относящейся к АЭС. На наш взгляд, такая модель может рассматриваться как базовая – она, при решении поставленной задачи верна в первом приближении, но не учитывает некоторые дополнительные (специфические) условия функционирования таких сложных (многокомпонентных и многопараметрических) нестационарных объектов как энергоблоки АЭС, которые характеризуются нелинейной динамикой реагирования на внешние воздействия [12].

Для усовершенствования базовой модели и повышения степени ее адекватности реальным условиям эксплуатации АЭС, на основе информационных материалов, являющихся частью современного уровня техники и используемых нами в данной работе, было проведено предварительное экспериментальное исследование, результаты которого привели к пониманию возможностей разработки усовершенствованной модели.

Установлено, что в первую очередь запаздывание может быть связано с переподготовкой контингента специалистов и обновлением «антивирусного» программного обеспечения, то есть с организационно-техническими обстоятельствами. Анализируя различные математические модели из числа рассмотренных, можно констатировать, что накладываемые при моделировании граничные условия ранее должным образом не учитывали фактор запаздывания в кинетике поступления и отражения угроз информационной безопасности в системе физической защиты АЭС, но для повышения адекватности моделирования должны в полной мере учитываться.

Кроме того, были выполнены опытные аналитические исследования, в которых – как еще один модифицирующий фактор зависимости (1) – рассматривалось временное запаздывание [14] в системе «угроза – противодействие» (или, в техническом аспекте прикладной информатики, «ресурс нападения – ресурс защиты»). Действительно, подразделения физической защиты энергоблоков АЭС, укомплектование специалистами по системному и оперативному управлению и эксплуатации комплекса инженерно-технических средств, происходит заблаговременно до начала монтажа и наладки автоматизированной информационно-управляющей системы, и соответствующий персонал проходит обучение и проверку профессиональной пригодности еще до введения такой системы в эксплуатацию [3]. Такие меры, отвечающие замыслу комплексного обеспечения защиты, являются целесообразными и необходимыми, так как могут исключить злоумышленное использование закладных устройств – то есть скрытно установленных технических средств, которые способны создать угрозу для важной сигнальной информации. Подобные меры позволяют в значительной мере избежать установки также программных закладок – то есть тайно внедренных программ, которые создают угрозу информации, содержащейся в компьютерах. Во многих случаях такой подход позволяет избежать инсталляции «компьютерных вирусов» – программных продуктов, которые могут неконтролируемо размножаться и распространяться, и обладают способностями к нарушению целостности информации, повреждению программного обеспечения

и (или) изменению режима работы вычислительной техники в составе информационно-управляющей системы. Описанные организационные меры неизбежно концептуально предусматривает определенное запаздывание в системе «угроза – противодействие». При этом, и фактор запаздывания, и другие модифицирующие факторы могут учитываться в комплексе для повышения адекватности (достоверности) моделирования.

Указанные обстоятельства приводят, на наш взгляд, к необходимости в задачах прикладной информатики при моделировании процессов кинетики информационных угроз, направленных на АЭС, использовать уравнение Хатчисона – как модификацию ранее использовавшихся моделей. Исходя из изложенного, с учетом времени запаздывания τ числа воздействий $x(t)$ на защищаемый объект, может быть предложено использование такой зависимости:

$$\frac{dx}{dt} = r_i^m \left(1 - \frac{x(t-\tau)}{K_i}\right) x(t). \qquad (2)$$

Модель, представленная зависимостью (2), может быть использована при оценке эффективности системы физической защиты объектов атомной энергетики, поскольку она учитывает реальные условия их эксплуатации, связанные с фактором запаздывания технологически важных информационных событий.

Как с научной, так и с практической точки зрения небезынтересно отметить, что колебательный процесс, если он развивается при наличии действия фактора запаздывания защитной реакции на создающее угрозу внешнее воздействие, может, при определенных обстоятельствах, привести к неустойчивому колебательному процессу. Колебательная неустойчивость может сопровождаться запредельно ожидаемым ростом кибератак. Прогнозирование такого риска является при моделировании интенсивности кибератак стратегически важным [15]. Очевидно, что возникновение колебаний возможно лишь после точки перегиба кривой, где вторая производная функциональной зависимости $x(t)$ меняет знак. Поэтому в рамках рассматриваемого моделирования методически необходимой является регулярная проверка изменения знака зависимости:

$$\ddot{x} = r^m \dot{x} - 2\gamma x\dot{x} = \gamma\dot{x}\left(\frac{r^m}{\gamma} - 2x\right) = \gamma\dot{x}\left(K - 2x\right). \qquad (3)$$

Данное положение учитывалось в ходе экспериментирования, методически дополнившего теоретические разработки.

4 ЭКСПЕРИМЕНТЫ

План проведения экспериментов включал качественный и поэтапный количественный анализ предложенных модельных зависимостей. При этом в ходе экспериментальной проверки теоретических положений использовалась заимствованная нами модификация программы расчетов, разработанная в [9] на основе блок-схемы Simulink для модели Лотки-Вольтерры [13].

С учетом ограниченной фактической базы данных по статистике кибератак на объекты атомной энергетики (поскольку моделирование процесса организованных угроз относится не к прошедшему времени, а к настоящему и будущему) нами в рамках качественной оцени модельных зависимостей сначала был предпринят пилотный (объектно-ориентированный, на основе ограниченной выборки событий) эксперимент, в котором организованное усиление противодействия информационно защищаемого объекта, как и ожидалось, сопровождалось спадом интенсивности поступления информационных атак. Акты противодействия поступавшим атакам формировались в классическом формате «хищник–жертва» на основе процедур, апробированных в области социальной динамики взаимодействия противостоящих объектов, разделенных дистанционно (но не информационно).

На следующем этапе был проведен дополнительный анализ предложенных модельных зависимостей с привлечением пилотных экспериментальных исследований. Этот этап эмпирического анализа был связан с изучением изменений интенсивности $x(t)$ на расширенном (открытом) временном интервале. Сопоставление с известными численными данными, полученными ранее в области нелинейной динамики [9], позволили в ходе экспериментов проверить предположение о возможности переноса закономерностей кинетики отражения угроз в экосистеме «популяция хищников – популяция жертв», описываемых моделью Лотки-Вольтерры в рамках теории борьбы за существование, на технические объекты, исследуемые в данной работе. Этому способствовала формализация, которую обеспечивает подход, основанный на компьютерном (численном) моделировании.

В ходе экспериментирования учитывалось запаздывание, которое может быть связано с «человеческим фактором» и процедурой принятия решений, имеющими отношение к защите информации на АЭС. В ходе экспериментов проверка (знаковая оценка) выражения (3) позволяла установить значения времени для первой точки перегиба $x(t)=K_i/2$, и подготовиться к возможности упреждения более активного (ускоренного) повышения интенсивности информационных угроз в ожидании последующих точек перегиба модельной кривой [16] или к достижению значениями $x(t)$ экстремального изменения.

5 РЕЗУЛЬТАТЫ

Результаты качественной и количественной экспериментальной проверки показали, что спад интенсивности кибернетических угроз является закономерным. Опытным путем было установлено, что он может быть связан с сокращением «информационного ареала» субъектов, заинтересованных в организации угроз (например, – вследствие изменения и перераспределения сил влияния) и с изменением мотивации «агрессора», что нами учитывалось при моделировании. Результаты исследования показали, что эти обстоятельства имеют прямое отношение к информационному пространству, в котором функционирует атомная энергетика с учетом временных циклов работы энергоблоков АЭС. Характерной особенностью экспериментально полученных результатов, отображенных точками, определяющими кривую, которая показана на рис. 3 (наряду с аналитическими зависимостями, показанными сплошными линиями), является экстремум – максимум интенсивности информационных атак на защищаемый объект.

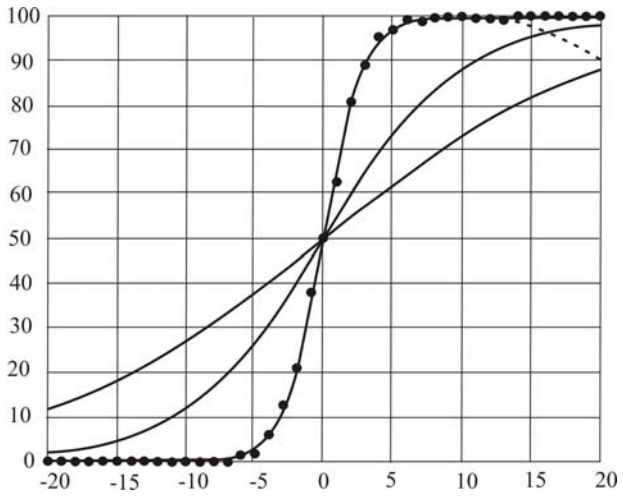

Рисунок 3 – Варианты функциональных зависимостей интенсивности кибератак на объекты атомной энергетики (ось абсцисс – время в годах, ось ординат – доля максимальной интенсивности в процентах)

Экстремальный характер модельной зависимости, связанный с трансформацией логистической кривой не только учитывает реальные условия осуществления угроз, направленных на защищаемый (противодействующий) объект, но и указывает на то, что имеется возможность прогнозировать значение времени (например, на основе тривиальной теоремы Ферма об исследовании функции на экстремум), после которого интенсивность кибератак должна начать снижаться. Это важно в связи с тем, что можно заблаговременно выяснить – когда появляется дополнительный ресурс времени на усовершенствование и обновление информационно-технических возможностей в системе физической защиты объекта для противодействия внешним угрозам и наращивания емкости защитного потенциала.

Результаты пилотных экспериментов и результаты последующего сопоставительного анализа, подтвердившие адекватность предложенного подхода к моделированию, позволяют выполнить перенос полученных закономерностей на техническую систему в области информационной безопасности «ресурс нападения – ресурс защиты» в условиях работы различных объектов атомной энергетики. Результатом экспериментов стало также понимание значимости колебаний параметра $x(t)$, для адекватного прогнозирования процесса поступления кибератак на АЭС и соответствующего противодействия информационным угрозам. То, что, согласно результатам экспериментов, колебательный процесс может действовать как модифицирующий фактор формы логистической кривой, отвечающей зависимости (1) в прикладных задачах информатики и в области задач физической защиты АЭС, создает предпосылки для правильной организации информационной защиты энергоблоков АЭС на протяжении всего времени их функционирования, с учетом продления проектного срока службы до 60 лет.

6 ОБСУЖДЕНИЕ

В порядке обсуждения результатов выполненной работы, следует отметить, что анализ результатов проведенных теоретических и экспериментальных исследований показывает, что предложенные модельные зависимости при анализе кинетики кибератак и соответствующего их блокирования или активного отражения в системе информационной безопасности энергоблоков АЭС представляются наиболее адекватными из числа аналогов, известных в прикладной информатике.

Предложенный подход, целесообразность которого нашла подтверждение в ходе теоретических и экспериментальных исследований, позволяет распространить примененную математическую идеологию на область действия других факторов влияния на интенсивность кибератак, направленных на АЭС.

Так, к факторам информационной безопасности АЭС, особенности влияния которых являются менее значимыми и требуют отдельных дополнительных (уточняющих) исследований, относится то, что каждый из фигурирующих в модельных зависимостях операндов в общем случае является нестационарным и зависит от многих, зависящих от времени показателей, специфичных для объектов атомной энергетики (срок ввода в эксплуатацию, срок службы, коэффициент использования установленной мощности, стоимостные показатели и др.). Это обстоятельство может быть учтено в ходе дальнейших исследований.

Необходимо также заметить, что анализ устойчивости колебательных процессов $x(t)$ и запасов устойчивости этих процессов представляется отдельной задачей, интересной как с научной, так и с практической точки зрения. Эта задача рассматривается авторами в других публикациях [17, 18] и не является предметом данной работы, но, на наш взгляд, должна быть здесь упомянута в порядке обсуждения.

ВЫВОДЫ

Предложен поход к решению научной проблемы прикладной информатики, относящейся к выбору адекватной модельной зависимости для анализа кинетики кибернетических атак на программно-технический комплекс информационной безопасности в составе системы физической защиты АЭС. Установлена возможность повышения достоверности моделирования. Рекомендуемые к использованию модельные зависимости впервые адаптированы к условиям эксплуатации объектов атомной энергетики, учитывают факторы противодействия угрозам и обстоятельства, связанные со специфическим временным запаздыванием. Определены новые пути совершенствования базовых математических моделей для их практического применения в технологиях обеспечения физической защиты АЭС.

Научная новизна заключается в развитии и уточнении ранее не принятых во внимание положений в области прикладной информатики, в порядке применения их к системам физической защиты АЭС, а именно: существует возможность как экстремального, так и колебательного характера зависимости интенсивности кибернетических атак, направленных на систему программно-технических средств информационной безопасности АЭС; адекватно адаптированное моделирование позволяет предположить реальность развития неустойчивого колебательного процесса в системе «нападение – защита» и дает возможность превентивной оценки соответствующих запасов устойчивости.

Полученные научные и практические результаты могут позволить при моделировании кинетики возникновения и отражения внешних кибернетических атак, направленных на систему физической безопасности АЭС, оценивать время наступления ожидаемых изменений текущей зависимости кибератак и использовать эти знания для организационно-технической подготовки средств защиты и заблаговременного упреждения IT-угроз.

БЛАГОДАРНОСТИ

Работа выполнена в рамках тематики этапа «Підвищення ефективності, надійності та безпеки роботи, в тому числі радіаційної, основного та допоміжного обладнання АЕС» в рамках госбюджетной работы «Дослідження можливостей удосконалення сучасних енерготехнологій і подальшої модернізації основного та допоміжного обладнання АЕС» (№ гос.регистрации 0116U004924), выполняемой на кафедре «Атомные электростанции» Одесского национального политехнического университета.

Авторы выражают благодарность коллегам – доценту кафедры информатики и управления защитой информационных систем В. Г. Кононовичу и начальнику службы физической защиты ВП «Рівненська АЕС» И. Я. Дерлюку – за предоставленную нам возможность ознакомления с опубликованными материалами, которые были использованы в наших исследованиях и учтены в процессе работы над данной статьей, а также за обсуждение вопросов, имеющих отношение к физической безопасности АЭС и общим аспектам информационной безопасности технических объектов.

СПИСОК ЛИТЕРАТУРЫ

1. Рекомендации по физической ядерной безопасности, касающиеся физической защиты ядерных материалов и ядерных установок (INFCIRC/225/REVISION 5) / Серия изданий МАГАТЭ по физической ядерной безопасности, № 13. – МАГАТЭ, Вена. – 2012. – 69 с.
2. Закон України «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» от 19 октября 2000 р. №2064-III // Відомості Верховної Ради України (ВВР), 2001. – №1, ст. 18.
3. Наказ Державної інспекції ядерного регулювання України 05.12.2011 №176 / Зареєстровано в Міністерстві юстиції України 23 грудня 2011 р. за №1505/20243.
4. Советов Б. Я. Информационные технологии : учеб. для ВУЗов / Б. Я. Советов, В. В. Цехановский. – М. : Высш. шк., 2003. – 263 с.
5. Киселев В. В. Кибервойна как основа гибридной операции / В. Киселев, А. Костенко // Армейский сборник. – 2015. – Т. 257, № 11. – С. 3–6.
6. Головко В. В. Первая кибернетическая атака на объект атомной энергетики / В.В. Головко // Наука и техника. – 2016. – № 4. – С. 74–78.
7. Келети Т. Основы ферментативной кинетики / Т. Келети. – М. : Мир, 1990. – 350 с.
8. Про внесення змін до Закону України «Про інформацію» // Відомості Верховної Ради України (ВВР). – 2011, № 32, ст. 313.
9. Кононович І. В. Динаміка кількості інцидентів інформаційної безпеки / І. В. Кононович // Інформатика та математичні методи в моделюванні. – 2014. – Т. 4, № 1. – С. 35–43.
10. Мышкис А. Д. Элементы теории математических моделей. Изд. 2-е, испр. / А. Д. Мышкис. – М. : Едиториал УРСС, 2004. – 191 с.
11. ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення.
12. Малинецкий Г. Г. Современные проблемы нелинейной динамики / Г. Г. Малинецкий, А. Б. Потапов. – М. : Эдиториал УРСС, 2000. – 326 с.
13. Трубецков Д. И. Феномен математической модели Лотки-Вольтерры и сходных с ней / Д. И. Трубецков // Известия высших учебных заведений. Прикладная нелинейная динамика. – 2011. – Вып. 2, Т. 19. – С. 69–88.
14. Долгий Ю. Ф. Математические модели динамических систем с запаздыванием : учеб. пос. / Ю. Ф. Долгий, П. Г. Сурков. – Екатеринбург : Изд-во Урал ун-та, 2012. – 122 с.
15. Гайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Гайворонський, О. М. Новіков. – К. : Видавнича група ВНУ, 2009. – 608 с.
16. Богуш В. М. Теоретичні основи захищених інформаційних технологій : навч. посіб. / В. М. Богуш, О. А. Довидьков, В. Г. Кривуца. – К. : ДУІКТ, 2010. – 454 с.
17. Деревянко О. В. Предаварийные физические процессы и надежный теплоотвод в ядерных энергоустановках : монография / О. В. Деревянко, А. В. Королев, А. Ю. Погосов. – Одесса : Наука и техника, 2014. – 268 с.
18. Погосов О. Ю. Додаткові технічні можливості для удосконалення систем безпеки АЕС і зниження ризику негативного впливу об'єктів ядерної енергетики на довкілля / О. Ю. Погосов, О. В. Дерев'янко // Ядерна енергетика та довкілля. – 2016. – №1 (7). – С. 13–16.

Статья поступила в редакцию 16.01.2017.
После доработки 06.02.2017.

Погосов О. Ю.[1], Дерев'янко О. В.[2]

[1]Д-р техн. наук, професор, професор кафедри атомних електричних станцій Інституту енергетики і компьютерно-інтегрованих систем управління Одеського національного політехнічного університету, Одеса, Україна

[2]Канд. техн. наук, старший викладач кафедри атомних електричних станцій Інституту енергетики і компьютерно-інтегрованих систем управління Одеського національного політехнічного університету, Одеса, Україна

МОДЕЛІ ПРИКЛАДНОЇ ІНФОРМАТИКИ ВРАХУВАННЯ КІНЕТИКИ КІБЕРНЕТИЧНИХ ЗАГРОЗ В СИСТЕМІ ФІЗИЧНОГО ЗАХИСТУ АЕС

Актуальність. Розглянуто актуальні підходи до превентивних оцінок і математичного моделювання процесів кібернетичних атак і надходження зовнішніх техногенних інформаційних загроз, які можуть бути спрямовані на систему фізичного захисту енергоблоків сучасних атомних електричних станцій.

Мета роботи – адаптація відомих математичних моделей кінетики кібератак для використання в системі інформаційної безпеки та фізичного захисту АЕС до сучасних і прогнозованих умов.

Метод. Запропоновано метод адаптації модельних залежностей, що відображають кінетику кібератак умов експлуатації об'єктів атомної енергетики, що захищаються. Для вдосконалення модельних залежностей запропоновано модифікувати класичну функцію Ферхюльста і при математичному моделюванні кібернетичних атак на об'єкти атомної енергетики використовувати відповідну трансформацію логістичної кривої, яка має характерну особливість у вигляді чітко вираженого максимуму.

Результати. Передбачено, що модельна залежність потоку зовнішніх по відношенню до АЕС кібернетичних загроз може характеризуватися чергуванням мінімумів і максимумів, що вказує на можливість коливального характеру процесу, що розвивається. Також висунута і обгрунтована гіпотеза про те, що система фізичного, і зокрема, кібернетичного, захисту АЕС може характеризуватися тимчасовим запізненням, що з урахуванням можливого коливального характеру процесу надходження інформаційних загроз створює передумови для розвитку коливальної нестійкості. Результати, отримані в ході досліджень, носять прикладний характер, можуть бути

використані для проведення широкомасштабних експериментів і прогнозування параметрів спрямованих на АЕС можливих кібернетичних загроз з метою їх попередження та превентивного забезпечення інформаційної безпеки сучасних ядерних енерготехнологій.

Висновки. Рекомендовані до використання модельні залежності вперше адаптовані до умов експлуатації об'єктів атомної енергетики, враховують фактори протидії загрозам і обставини, пов'язані зі специфічним тимчасовим запізненням.

Вперше показано, що існує можливість як екстремального, так і коливального характеру залежності інтенсивності кібернетичних атак, спрямованих на систему програмно-технічних засобів інформаційної безпеки АЕС. Новий підхід дозволяє припустити реальність розвитку нестійкого коливального процесу в системі «напад - захист» і дає можливість превентивної оцінки відповідних запасів стійкості.

Практична значущість полягає в тому, що отримані результати дозволяють реалістично оцінювати час настання очікуваних змін поточної залежності кібератак і використовувати ці знання для організаційно-технічної підготовки засобів захисту і завчасного попередження ІТ-загроз.

Ключові слова: прикладна інформатика, інформаційна безпека, фізичний захист АЕС, математичне моделювання кібернетичних атак на об'єкти атомної енергетики.

Pogosov A. Yu.[1], Derevianko O. V.[2]

[1]Dr.Sc., Professor, Professor of Nuclear Power Plants Department, Odessa National Polytechnical University, Odessa, Ukraine

[2]Ph.D., Senior Lecturer of Nuclear Power Plants Department, Odessa National Polytechnical University, Odessa, Ukraine

APPLIED INFORMATICS MODEL OF KINETICS ACCOUNTING OF CYBERNETIC THREATS IN NPP PHYSICAL PROTECTION SYSTEM

Context. The topical approaches to preventive estimations and mathematical modeling of cyber attacks processes and supply of external technological informational threats were considered, which may be directed on the physical security system of modern nuclear power plant units.

Objective – is an adaptation of known mathematical models of cyber attacks kinetics for use in the system of information security and physical protection of nuclear power plants to modern and foreseeable conditions.

Method. The method of model dependencies adaptation was proposed, which reflects the kinetics of cyberattacks to the modern operating conditions of protected nuclear facilities was proposed. To improve the model dependencies it was proposed to modify the classic Ferhulst function and, in mathematical modeling of cyber attacks on nuclear power facilities, to use the appropriate transformation of the logistic curve, which has distinctive feature of a well-defined maximum.

Results. It was predicted that the model dependence of flow external to NPP cyber threats can be characterized by the alternation of maxima and minima, which indicates the possibility of an oscillatory character of the developing process. Also was put forward and substantiated the hypothesis that the system of physical and, in particular, cybernetic, NPP protection can be characterized by a time lag that in view of possible oscillatory character of information threats admissions process creates the preconditions for the development of oscillatory instability. The results obtained in the research are of applied nature, they can be used to carry out large-scale experiments and forecasting parameters of possible cyber threats aimed at the NPP for the purpose of pre-emption and preventive maintenance of information safety of modern nuclear energy technologies.

Conclusions. Recommended for use model dependences were first adapted to the conditions of operating conditions of nuclear power facilities, take into account the factors to counter threats and circumstances associated with a specific time delay.

It was shown for the first time that there is an opportunity both extreme and oscillatory dependence nature of the cyber attacks intensity, which are focused on software and hardware system of NPP information safety. The new approach allows to assume the reality of the unstable oscillation process in the "attack – defense" system and provides an opportunity of preventive assessment of the stability stocks.

The practical significance lies in the fact that the results allow to realistically assess the time of onset of expected cyber attacks current dependence changes and to use this knowledge for organizational and technical preparation of remedies and early anticipation of IT-threats.

Keywords: applied computer science, information security, NPP physical security, mathematical simulation of cyber attacks on nuclear power facilities.

REFERENCES

1. Recommendations on Nuclear Security, on the physical protection of nuclear materials and nuclear facilities (INFCIRC/225/ REVISION 5) / IAEA Nuclear Security Series, № 13, IAEA, Viena, 2012, 69 p.
2. The Law of Ukraine "On the physical protection of nuclear facilities, nuclear materials, radioactive waste and other sources of ionizing radiation" on October 19, 2000. №2064-III, *Vidomosti Verkhovnoi Rady Ukrainy (VVR),* 2001, No. 1, st. 1).
3. Order of the State Nuclear Regulatory Inspectorate of Ukraine 05.12.2011 №176 / Registered with the Ministry of Justice of Ukraine 23.12.2011, №1505/20243.
4. Sovetov B. Ya., Cekhanovsky V. V. Informacionnye tekhnologii : Ucheb. Dlia VUZov. Moscow, Vyssh. Shk., 2003, 263 p.
5. Kiseliov V., Kostenko A. Kibervojna kak osnova gibridnoj operacii, *Armejskij sbornik,* 2015, Vol. 257, No. 11, pp. 3–6.
6. Golovko V. V. Pervaia kiberneticheskaia atatka na ob'ekt atomnoj energetiki, *Nauka I tekhnika*, 2016, No. 4, pp. 74–78.
7. Keleti T. Osnovy fermentativnoj kinetiki. Moscow, Mir, 1990, 191 p.
8. Pro vnesennia zmin do Zakonu Ukrainy "Pro Informaciiu", *Vidomosti Verkhovnoi Rady Ukrainy (VVR),* 2011, No. 32, ст. 313.
9. Kononovych I. V. Dynamilka kil'kosti incydentiv informacijnoi bezpeky, *Informatyka ta matematychni metody v modeliuvanni.* Odesa, 2014. Vol. 3, No. 3, pp. 35–43.
10. Myshkis A. D. Elementy teorii matematicheskikh modelej. Izd. 2-e, ispr. Moscow, Editorial URSS, 2004, 191 p.
11. DSTU 2226-93 Avtomatyzovani systemy. Trminy ta vyznachennia.
12. Malineckij G. G., Potapov A. B. Sovremennye problem nelinejnoj dinamiki. Moscow, Editorial URSS, 2000, 326 p.
13. Trubeckov D. I. Fenomen matematicheskoj modeli Lotki-Volterry I skhodnykh s nej, *Izvestiia vysshikh uchebnykh zavedenij, Prikladnaia nelinejnaia dinamika,* 2011, Vyp. 2, Vol. 19, pp. 69–88.
14. Dolgij Yu. F., Surcov P. G. Matematicheskie modeli denamicheskikh system s zapazdyvaniem : ucheb. posobie. Ekaterinburg: Izd-vo Uralskogo un-ta, 2012, 122 p.
15. Gajvorons'kyj M. V., Novikov O. M. Bezpeka informacijno-kommunikacijnykh system. Kiev, Vydavnycha grupa VNU, 2009, 608 p.
16. Bogush V. M., Dovyd'kov O. A., Kryvutsa V. G. Teoretychni osnovy zakhyschenykh informatsijnykh tekhnologij : navch. posibn. Kiev, DUIKT, 2010, 454 p.
17. Derevianko O. V. Koroliov A. V., Pogosov A. Yu. Predavarijnye fizicheskie protsessy i nadiozhnyj teplootvod v iadernykh energoustanovkakh : monographiia. Odessa, Nauka i tekhnika, 2014, 268 p.
18. Pogosov O. Yu., Derevianko O. V. Dodatkovi tehnichni mozhlyvosti dlia udoskonalennia system bezpeky AES i znyzhennia ryzyku negatyvnogo vplyvu ob'ektiv iadernoi energetyky na dovkillia, *Yaderna energetyka ta dovkillia,* 2016, No. 1(7), pp. 13–16.