Scientific and Practical Cyber Security Journal (SPCSJ) 6(1): 15-23 ISSN 2587- 4667
Scientific Cyber Security Association (SCSA)

РОЛЬ МОТИВАЦИОННОЙ ХАРАКТЕРИСТИКИ В ОНТОЛОГИИ КИБЕРБЕЗОПАСНОСТИ
ROLE OF MOTIVATIVE CHARACTERISTICS IN CYBER SECURITY ONTOLOGY

д.п.н., профессор РАЕ Козубцов Игорь Николаевич, Военный институт телекоммуникаций и информатизации имени Героев Крут, г. Киев, Украина
Doctor of Pedagogical Sciences, Professor of RAE, Igor Kozubtsov,Military institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine
к.т.н., Козубцова Леся Михайловна, Военный институт телекоммуникаций и информатизации имени Героев Крут, г. Киев, Украина
Candidate of Engineering Sciences, Lesya Kozbtsova,Military institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine
к.т.н., доцент Лещина Валерий Александрович, Луцкий национальный технический университет, г. Луцк, Украина
Candidate of Engineering Sciences, Associate Professor, Valery Leshchina Lutsk National Technical University, Lutsk, Ukraine

АННОТАЦИЯ. Актуальность темы исследований о необходимости обеспечения кибербезопасности информационных систем и технологий в образовании обусловлена постоянно возрастающей уязвимостью, а также скрытым рыском потери активов учебных заведений.

Основных аспекты работы. В статье поднимается вопрос о необходимости рассмотрения обеспечения кибербезопасности информационных систем и технологий в образовании. Установлено, что в данное время исследователями не приделано надлежащего внимания вопросу обеспечения кибербезопасности в проектируемых информационных системах и технологиях в сфере образования.

Научная новизна. Научная новизна темы заключается в постановке задании о необходимости решение научно-практической задачи обеспечения кибербезопасности информационных систем и технологий в образовании.

КЛЮЧЕВЫЕ СЛОВА: *кибербезопасность, мотивация, характеристика, онтология, киберпротивостояние*.

ABSTRACT. The relevance of the research topic on the need to ensure the cybersecurity of information systems and technologies in education is due to the constantly increasing vulnerability, as well as the hidden risk of losing assets of educational institutions.

The main aspects of the work. The article raises the question of the need to consider the provision of cybersecurity of information systems and technologies in education. It is established that at this time, researchers have not paid proper attention to the issue of ensuring cybersecurity in the projected information systems and technologies in the field of education.

Scientific novelty. The scientific novelty of the topic lies in the formulation of a task about the need to solve the scientific and practical problem of ensuring the cybersecurity of information systems and technologies in education.

KEYWORDS: *cybersecurity, education, information system, technology, destructive information influence, cyber security, methodology.*

ВВЕДЕНИЕ

В настоящее время в многочисленных нормативных документах по вопросам обороны и безопасности любого государства ведущее место отводится проблеме противодействия киберугроз (КУ). Например, в [1; 2] КУ отнесены к актуальным угроз национальной безопасности государства, а создание системы кибербезопасности (КБ) и защиту от кибернетических атак определен неотложными задачами.

Анализ причин возникновения проблемы показал, что такими причинами являются:

наличие негативно настроенных группировок, которые желают реализации противоправных действий в кибернетическом пространстве путем нарушения целостности, доступности и конфиденциальности информации для и нанесения вреда информационным ресурсам и телекоммуникационным системам;

группировка программистов типа «хакер» гораздо быстрее создает вредоносное программное обеспечение нежели обновляется антивирусное (программное обеспечение);

эффективность применения информационных технологий и вредоносного программного обеспечения в

кибернетическом пространстве в интересах осуществления военно-политического и силового воздействия противоборства, враждебной информационной / кибероперации, поддержки терроризма и проведения хакерских атак.

Именно в ходе создания и настройки системы связи происходит выявление и обеспечение защиты от стремительное развитие кибернетических угроз.

Современные средства киберзащиты информации принимаются на вооружение с определенными трудностями, в связи с отсутствием достаточного финансирования.

Поэтому, учитывая выше изложенного, по нашему мнению, возникла необходимость в данной работе рассмотреть отдельный аспект, который связан с необходимостью изучения мотивационной характеристики защитника киберпространства что бы своевременно исключать смену позиции защитник-нарушитель.

АНАЛИЗ ПОСЛЕДНИХ ИССЛЕДОВАНИЙ И ПУБЛИКАЦИЙ ПО ДАННОМУ НАПРАВЛЕНИЮ

Автор работы [3] при создании модели угроз информации и механизма ее эффективной защиты описывают модель нарушителя, как абстрактное формализованное или неформализованные описание действий нарушителя, который отражает его практические и теоретические возможности, априорные знания, время, место действия и тому подобное. Даная работа вдохновила на продолжения авторских исследований. Так в работе [4] обращено внимание на мотивационный портрет участники кибернетического противостояния, который меняется от множества условий. В связи с этим обстоятельством акцентировано внимание участников научно-практической конференции «Применение информационных технологий в подготовке и деятельности сил охраны правопорядка» (Харьков, 17-18 марта 2016 г.) на необходимость проведения исследований по более подробному изучению мотивационной характеристики военнослужащих при допуске их к кибернетическому противостоянию [5].Таким образом, не решенным вопросом является обоснование моделей участников киберпространства на основе классификации, что бы упростило процедуру математического расчета, а также сделало невозможным возникновение парадокса в случае отсутствия каких-либо расчетных данных.

ЦЕЛЬ СТАТЬИ

Раскрыть основные результаты исследования вопроса о необходимости изучения мотивационной характеристики участников противостояния в киберпространстве, от которой в первую очередь зависит изменения онтологии кибербезопасности.

ОСНОВНОЙ РЕЗУЛЬТАТ ИССЛЕДОВАНИЯ

Наше исследование основывается на предложенной стратегии игры в киберпространстве [6] и модели [7] при оценке устойчивости функционирования критическая информационная инфраструктура. В виду того, что данная модель используется в исследовании проблемы киберживучести энергосистемы Украины [8], тогда можно утверждать о ее адекватности и для нашего рассматриваемого случая. Таким образом, нами синтезировано графическая модель возможного противоборствия в киберпространстве.

В работе [9] автор четко дает понятие кибератаки, как формы враждебных (противоправных) действий в киберпространстве; действия, направленные против кибернетических систем, информационных ресурсов или информационной инфраструктуры для достижения какой-либо цели и осуществляемые при помощи специальных программно-аппаратных средств и приемов (способов) воздействия.

В контексте данной работы не будем рассматривать задачи, формы и способы ведения войн в киберпространстве, исчерпывающая информации представлена в работе [10].

Для понимания киберпротивостояние приведем наглядный пример в виде рисунка (рис. 1). Однако, при внимательном рассмотрении модели, представленной на рис. 1, можно обратить внимание, что не отображается блок мотивации участников возможного противоборствия в киберпространстве.

В тоже время очень наглядно мотивационная характеристика, как условия, продемонстрировано в работе [11], можно несущественно изменив его таким образом, чтобы оно решал нашу задачу исследования. Конечный результат предлагается дополнить предложенную ранее усовершенствованная онтология кибербезопасности.

Рассматривая киберугрози в контексте государства следует рассмотреть общую классификация видов угроз кибербезопасности любого государства, систематизировав ее представим в табл. 1 и устойчивые к тенденциям развития киберугроз в мировом информационном пространстве [12].

Таблица 1 – Угрозы кибернетической безопасности государства

Вид угрозы	Краткое содержание (характеристика)
Кибервойна	Большинство стран мира активно наращивает свои потенциалы в сфере обороны в направлении усиления кибервозможностей ведения боевых действий и защиты от аналогичных действий со

	стороны противника, поскольку все более актуальными становятся новые киберугрозы. Внедрение ведущими странами современных кибервооружений превращает киберпространство в сферу ведения боевых действий, а в ближайшем будущем уровень обороноспособности страны будет определяться в т.ч. наличием у нее эффективных подразделений для ведения боевых действий в киберпространстве, способным противостоять киберугрозам в сфере обороны.
Кибертерроризм	Ряд отечественных предприятий, нарушение работы которых может представлять угрозу жизни и здоровью граждан, может стать потенциальной целью для осуществления террористических актов, в том числе - по применению современных информационных технологий. Все большее распространение получает политически мотивированная деятельность в киберпространстве групп активистов (хактивистов), которые осуществляют атаки на правительственные и частные сайты, приводит к нарушениям работы информационных ресурсов, а также репутации и материальных убытков
Кибершпионаж	Не меньшей угрозой является совершение противоправных действий в ущерб третьим странам, которые осуществляются с использованием отечественной информационной инфраструктуры, угрожающих устойчивому и безопасному функционированию национальных информационно-телекоммуникационных систем
Киберпреступность	Преступления с использованием современных информационно-телекоммуникационных технологий становятся все обычной практикой в жизни украинских граждан. Больше всего внимание преступников сосредоточена на попытках нарушения работы или несанкционированного использования возможностей информационных систем государственного, кредитно-банковского, коммунального, оборонного и производственного секторов

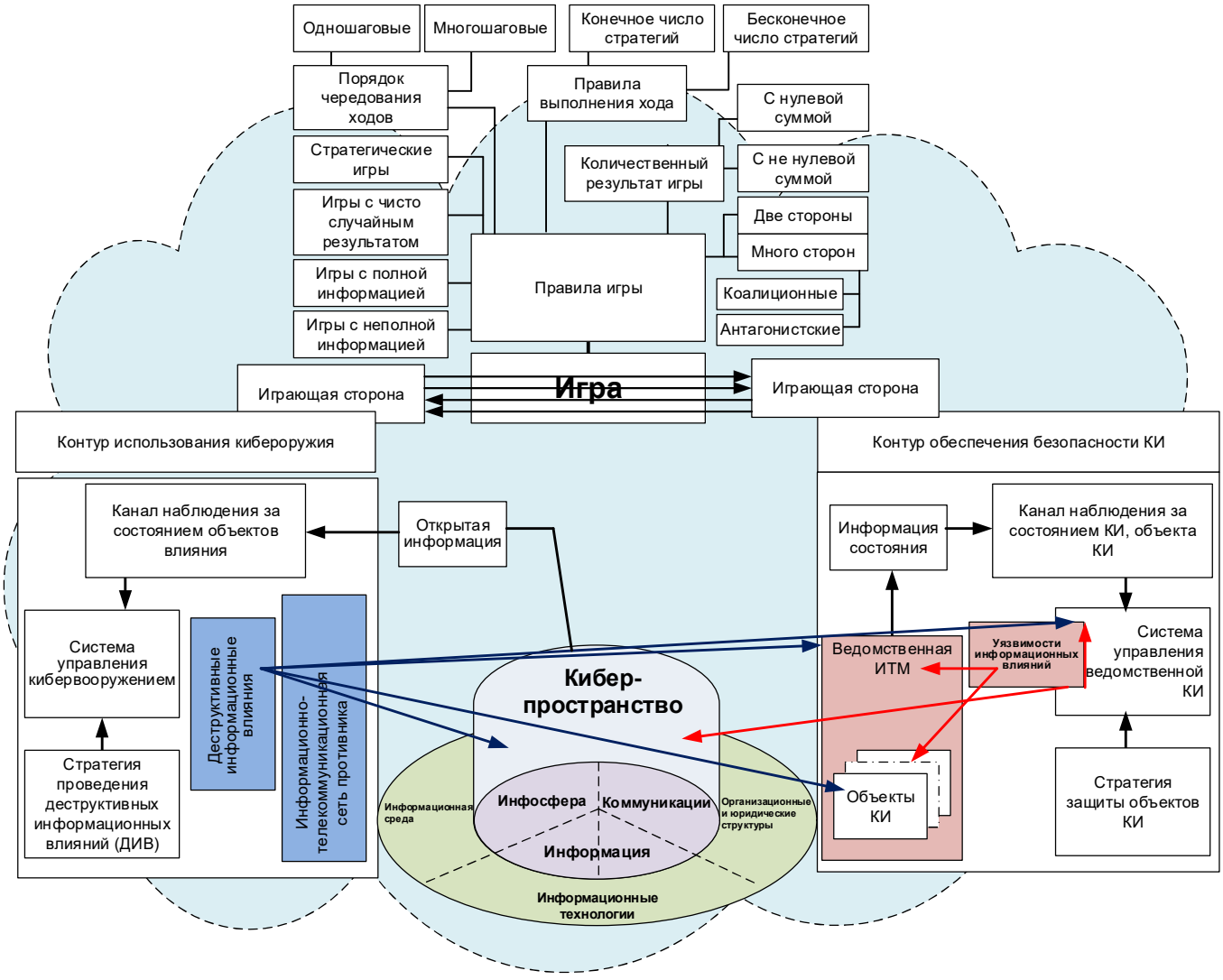

Рис. 1 – Модель противостояния в киберпространстве

Для разработки действенных путей борьбы с источниками киберугроз необходимо выяснить мотивацию всех участников киберпространства. По природе мотивы могут быть совершенно разными: от полного их отсутствия, стихийных бедствий, экономических и политических преимуществ в целенаправленных воздействий вовремя кибервойны (табл. 2).

Таблица 2 – Источники угроз для информации

вид угроз	источники угроз	Мотивация источники угроз
Кибервойна	другие государства	Получение преимуществ во внешнеполитической, внешнеэкономической, военной и других сферах
Кибервойна	политические партии	Получение преимуществ в политической борьбе за власть
Кибертерроризм	преступные группировки	Получение политических, экономических преимуществ, нанесения ущерба
Кибершпионаж	субъекты хозяйствования	Получение преимуществ в конкурентной борьбе, экономические преимущества
Киберпреступность	физические лица	Самоутверждения, получения экономических преимуществ и финансовых вознаграждений
Киберпреступность	Ошибки персонала (умышленные, неумышленные)	Низкая квалификация работников; образа; измена; принуждение

Предоставим описание участников игры.

Авторы работы [12 с. 156] определили субъекты киберпространства только в общем виде не предоставив принадлежность к гражданству. А это, по нашему мнению, важно, поскольку правила поведения в кибернетическом пространстве определяется этическими нормами поведения и нормативно-процессуальным законодательством страны. Зато нормативно-процессуальное законодательство стран мира имеет различия, которые постепенно устраняет глобализационный процесс.

Условно их можно сгруппировать в три группы: граждане страны, люди без гражданства, иностранные граждане. Согласно им, смоделируем следующие модели:

модель нарушителя информационно-киберпространства;

модель защитника информационно-киберпространства.

Также следует условно представить, что воздействие может осуществляться человеком как извне государства, так и изнутри.

Каждая из групп имеет за разногласиями нормативно-процессуальным законодательством страны, в которой она находится и собственных убеждений этическими нормами поведения.

Приближенную классификацию участников кибернетического пространства представлено в табл. 3.

Таблица 3 – Классификация участников кибернетического пространства

Участники киберпространства	уровень сети	Категория пользователя	Модель поведения	
			защитника	нарушителя
граждане своей страны	сеть внутренняя закрытая	военнослужащие; военнослужащие других воинских (силовых) формирований; работники военных (силовых) формирований	+	+ / –
	сеть внутренняя (корпоративная)	граждане своей страны (члены корпорации) нерезиденты (члены корпорации)	+	+ / –
	сеть Интернет	все перечисленные категории граждане	+	+ / –
иностранные граждане	сеть внутренняя закрытая (в пределах своего государства)	граждане страны, которым предоставлен допуск и доступ к сети	– / +	+
	сеть внутренняя (корпоративная)	граждане одной страны (члены корпорации) нерезиденты и резиденты (члены корпорации)	– / +	+
	сеть Интернет	все перечисленные категории граждане	– / +	+
лица без гражданства (находящихся внутри страны)	сеть внутренняя закрытая	доступ запрещен	– / +	+
	сеть внутренняя (корпоративная)	члены транснациональных корпорации	– / +	+
	сеть Интернет	все перечисленные категории граждане	– / +	+
лица без гражданства	сеть внутренняя закрытая	доступ запрещен	– / +	+

(находящихся за пределами страны)	сеть внутренняя (корпоративная)	члены транснациональных корпорации	– / +	+
	сеть Интернет	все категории граждане	– / +	+
провайдеры Интернета	ведущий	материальная мотивация	+	+ / –
	региональный	материальная мотивация	+	+ / –
	периферийный	материальная мотивация	+	+ / –
	проводной	материальная мотивация	+	+ / –
	(Беспроводной) сотовый	материальная мотивация	+	+ / –

Для построения игровой стратегии кибернетической безопасности выяснить вопрос при каких условиях участник кибернетического пространства принимает модель защитника, а при каких нарушителя. На этот вопрос можно частично найти ответ сразу выяснив факторы, влияющие, например, мотивация.

Условную классификацию мотивацию участников кибернетического пространства представлено в табл. 4.

Таблица 4 – Классификация мотиваций участников кибернетического пространства

Мотивации участников киберпространства	Дополнительная классификация	Модель		
		защитника	нарушителя	пользователя
материальные	телекоммуникационные компании	+ / –	+ / –	
	провайдер Интернета	+ / –	+ / –	
	абонент - пользователь	+ / –	+	+
духовные	абонент - пользователь	+	+ / –	+ / –
идейные	политические	+	+ / –	+ / –
	религиозные	– / +	+ / –	+ / –
	истинные патриоты	+	+	+ / –
	неискренни патриоты	– / +	+ / –	+ / –
	криминал	–	+	–
Устойчивое формирование мотивации, не поддается быстрому корректировке	любознательность	– / +	+	+
	энтузиасты	+	+	+ / –
	идиоты	–	+	–
профессиональные	разведчик	+	–	–
	шпион	–	+	–
Инсайдеры	все категории граждане	–	+	+ / –
Типичные условия и факторы влияния на мотивацию, побуждающих человека к правонарушению				
подкуп	все категории граждане	–	+	+ / –
шантаж	все категории граждане	–	+	+ / –
бюрократия	все категории граждане	+	+	+ / –
профессиональные	все категории граждане	+	+	+ / –
болезнь	все категории граждане	+	+	+ / –
особые потребности	все категории граждане	+	+	+ / –
Потребности по Маслоу: все категории граждане	все категории граждане	– / +	+ / –	+ / –
Потребности по Маслоу: все категории граждане	все категории граждане	– / +	+ / –	+ / –
Потребности по Маслоу: все категории граждане	все категории граждане	– / +	+ / –	+ / –
Потребности по Маслоу: все категории граждане	все категории граждане	– / +	+ / –	+ / –
Потребности по Маслоу: все категории граждане	все категории граждане	+ / –	–	+

Введя в таблицы 3 и 4 определенные условные сокращения и обозначения, можно математически сформировать матрицу параметров.

При разработке модели нарушителя киберпространства нами изучался опит построение таких моделей исчерпывающе представленных в работах М.М. Войтко [13], А.А. Конева [14], В.В. Семко [15] и других. С точки зрения рассматриваемой задачи интересен результат работы [13], в которой исследователь предложил рассматривать модель нарушителя в следующей математической форме так (1):

$$M_0 = \left(O_p, O_{\ln}, O_a\right) \quad (1)$$

где O_p – местоположение нарушителя;

O_{ln} – профессиональный уровень знаний и умений нарушителя;

O_a – сценарий возможного доступа O_{pn} – первичные знания нарушителя о системе.

Согласно работы [13] $O_p \in \{1, 2, 3\}$, где 1 – нарушитель внешний; 2 – нарушитель внутренний; 3 – преступная договоренность внутренних и внешних нарушителей, например, подкуп, шантаж.

Профессиональный уровень знаний и умений нарушителя $O_{ln} \in \{1, 2, 3\}$, где 1 – низкий уровень; 2 – средний уровень; 3 – высокий уровень.

Первичные знания нарушителя о системе КБ зависят от местоположения нарушителя относительно нее.

Однако автор работы [13] совершенно не учитывает мотивационной характеристики (МХ), как можно увидеть дальше модель в зависимости от этого параметра трансформируется в модель защитника КБ.

Все указанные в табл. 3 участники могут принимать модель защитника или нарушителя кибернетического пространства в зависимости от сложившейся внутренней характеристики мотивации.

В дальнейших исследованиях необходимо определить четко состав участников (организационную структуру) функциональные обязанности, сектор ответственности каждого участника, правила игры всех участников кибернетического пространства.

До сих пор не решенным вопросом является каким образом построить подобную мотивационную характеристику. Предположительно МХ имеет непосредственную связь с иерархической системой потребностей человека – пирамидой потребностей А. Маслоу [16]. В основе этой иерархии лежали наиболее насущные потребности (пища, вода, жилье), а на вершине – более высокие индивидуальные запросы (признание, самовыражение). Когда потребности самого низкого уровня удовлетворены хотя бы частично, человек начинает двигаться к удовлетворению потребностей другого и не обязательно следующего уровня иерархии. В каждый конкретный момент времени человек будет стремиться к удовлетворению той потребности, для нее важнее или сильной. Основной недостаток теории Маслоу сводится к тому, что ей не удалось учесть индивидуальные отличия людей. Исходя из прошлого опыта, один человек может быть больше заинтересована в самовыражении, в то время как поведение другого будет в первую очередь определяться потребностью в признании, социальными потребностями. Согласно результатов исследований [16] на психические (физиологические) потребности среднего гражданина удовлетворяются на 85%, экзистенциальные – на 70, социальные – на 50, престижные – на 40, самовыражения – на 10%. Статистика говорит, что только один-два процента людей стремится к вершине пирамиды Маслоу.

Что касается склонность всех категорий граждан можно с легкостью спрогнозировать вероятность наступления событий зная физиологическое положение страны или другие критерии по Маслоу.

Авторами [17] разработан принцип рефлексного управления, что нацелен на захват и удержание информационного превосходства над противником. На учет этого принципа акцентируют авторы монографии [18] поэтому игнорировать его неуместно. Цель принципа достигается путем управления личностью, если предложения внешней среды превышают ожидания личности. Модель представлена на рис. 2. Она напоминает модель рычагов, на чаше которых с одной стороны модель поведения защитника КБ, а на противоположной модель нарушителя КБ. Склонение человека к модели защитника или нарушителя КБ напрямую зависит от состояния мотивационной характеристики (МХ).

Отметим, что предложения внешней среды – это не только подкуп, шантаж, а еще выполнения задания, при этом человек делает правонарушения. Типичные условия и факторы влияния на мотивацию, побуждающих человека к правонарушению приведена в табл. 4. Следует обратить внимание на такой фактор как оценка уровня денежного обеспечения защитника КБ, а также чрезмерного бюрократического подхода допуска человека к системе КБ, условий ее эксплуатации, то есть создание деструктивных и некомфортных условий пользователю. Развивая данное направления исследования было подробней изучено и установлено дополнительные факторы, которые способствуют законопослушного гражданина к сознательному правонарушение т.е. с точки Закона стать нарушителем.

Таким образом, еще раз акцентируем внимание на то, что в результате законопослушный гражданин вынужден сознательно идти на правонарушение что бы выполнить задание руководства в установлений строк и надлежащим уровнем.

Рис. 2 – Инвариантная модель поведения участника киберпространстве

С учетом рис. 2 предложенная ранее усовершенствованная онтология кибербезопасности [19] примет дальнейшее развитие. Для этого изобразим логическое место предложенного алгоритма, результирующий результат отобразим на рис. 3.

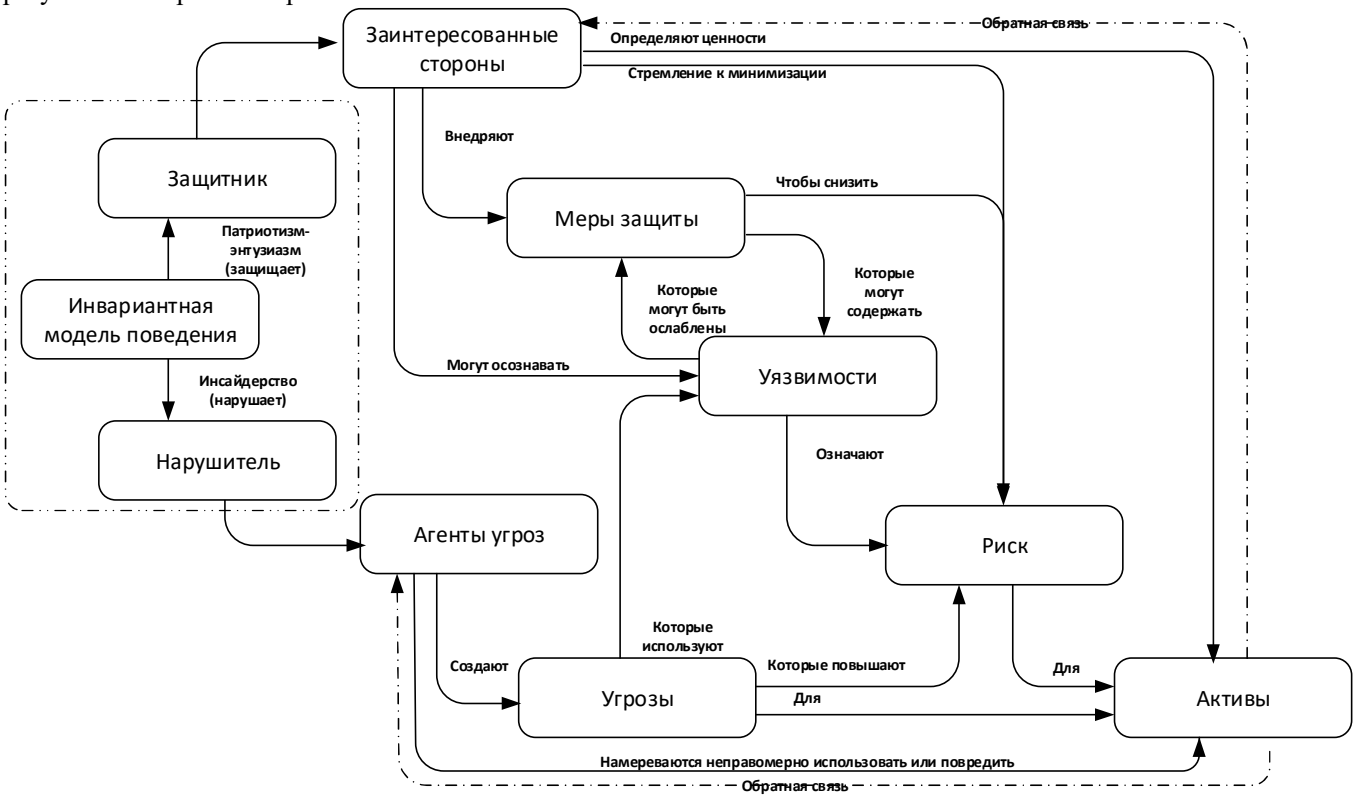

Рис. 3 – Функциональная зависимость онтология кибербезопасности

При моделировании следует учитывать человеческий фактор, который имеет место. Практика показывает, что на появление этого фактора влияют множество параметров, в том числе условия труда и отдыха. При определении степени влияния человеческого фактора на функционирование большой информационной системы нужно учитывать результаты о влиянии человеческого фактора на работоспособность информационных систем

[20].

ВЫВОДЫ

По результатам проведенного исследования можно сделать следующие выводи, которые вытекают из добавленных компонентов на функциональную зависимость онтология кибербезопасности.

1. Рационально необходимым является построения моделей нарушителя и защитника киберпространства с учетом мотивационной характеристики (портрета).

2. Созданием положительной мотивационной характеристики у защитников киберпространства уменьшает вероятность того, что ее защитник превратится в нарушителя киберпространства.

3. Для изучения мотивационной характеристики защитников киберпространства мы видим необходимость в подборе специальных психологических тестов. Такое тестирование позволит своевременное выявление потенциального инсайдера, его потребностей и склонности, а, следовательно, прогнозирования способности лиц к нарушениям в кибернетическом пространстве.

4. Мы намеренно не рассматривали нарушителей, имитирующие (создают) технические, вычислительные средства обработки информации (компьютера, ноутбуки, планшеты, мобильные приложения), поскольку они созданы биологической лицом (индивидуумом) исходя из собственной мотивационной характеристики. В таком случае они работают по определенному алгоритму. Задача может осложниться в будущем, когда искусственный интеллект начнет создавать собственное киберугрозу, что не исключается в будущем.

НАУЧНАЯ НОВИЗНА

В работе, в отличие от других, систематизировано и синтезировано в целостную систему последовательных явлений, а именно вытекающих от модели противостояния в киберпространстве и основных киберугроз до классификации классификация участников кибернетического пространства, их мотивационной характеристики до места и роли в усовершенствованной онтологии кибербезопасности. Эта информация в дальнейшем позволит упростить процедуру математического расчета, а также исключает возможность возникновения парадокса в случае отсутствия каких-либо расчетных данных.

ПЕРСПЕКТИВЫ ДАЛЬНЕЙШИХ НАУЧНЫХ ИССЛЕДОВАНИЙ

Перспективы дальнейших исследований целесообразно сосредоточить на основе обоснованных участников доступа к киберпространству и их мотивационной характеристике, приступить к разработке стратегии кибербезопасности обоснованной на игровом подходе.

СПИСОК ЛИТЕРАТУРЫ

1. Про рішення Ради національної безпеки і оборони України від 8 червня 2012 року «Про нову редакцію Воєнної доктрини України»: Указ Президента України № 390/2012. URL: http://zakon3.rada.gov.ua/laws/ show/390/2012.
2. Про Доктрину інформаційної безпеки України: Указ Президента України №514/2009. URL: http://zakon2.rada.gov.ua/laws/show/514/2009.
3. Капустян М.В., Орленко В.С., Хорошко В.О. Створення моделі загроз інформації та механізму її ефективного захисту // Вісник Національного університету «Львівська політехніка». 2006. № 551: Автоматика, вимірювання та керування. С. 58 – 63.
4. Козубцов І.М. Про мотиваційний портрет учасники кібернетичного протистояння // Актуальні проблеми розвитку науки і техніки: Матеріали першої міжнародної науково-технічної конференції. К.: ДУТ, 2015. С. 208 – 211.
5. Козубцов І.М., Козубцова Л.М., Живило Є.О., Куцаєв В.В. Про необхідність дослідження мотиваційної характеристики військовослужбовців при допуску їх до кібернетичного протистояння // Науково-практична конференція «Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку» (Харків, 17-18 березня 2016 р.). Харків: Національна академія Національної гвардії України, 2016. С. 35 – 36.
6. Козубцов І.М., Козубцова Л.М Стратегія гри в кібернетичному просторі // Матеріали Міжнародної науково-технічної конференції «Сучасні інформаційно-телекомунікаційні технології» (Київ, 17– 20 листопада 2015 р.). Київ. Державний університет телекомунікацій, 2015. Том ІІІ Розвиток інформаційних технологій. С. 52 – 54.

7. Минаев В.А., Королев И.Д., Зеленцова Е.В., Захарченко Р.И. Критическая информационная инфраструктура: оценка устойчивости функционирования // Радиопромышленность. 2018. Т. 28. №4. С. 59 – 67.
8. Гончар С.Ф., Герасимов Р.П., Ткаченко В.В. Дослідження проблеми кіберживучості Об'єднаної енергосистеми України // Міжнародний науково-теоретичний журнал "Електронне моделювання". 2019. Т.41. №1. С. 43 – 54.
9. Антонович П. О сущности и содержании кибервойны // Военная мысль. 2011. №7. С. 39 – 46.
10. Бурячок В.Л., Гулак Г.М., Хорошко В.О. Завдання, форми та способи ведення воєн у кібернетичному просторі // Наука і оборона. 2011. № 3 С. 35 – 42.
11. Гончар С., Леоненко Г., Юдін О. Загальна модель загроз безпеці інформації АСУ ТП // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: науково-технічний збірник. 2015. Вип. 1(29). С. 78 – 82.
12. Черняк О.Р., Федулов О.В. Тенденції розвитку кіберзагроз у світовому інформаційному просторі // Сучасні інформаційні технології у сфері безпеки та оборони. 2014. №1(19). С.155 – 158.
13. Войтко М.М. Побудова узагальненої моделі загроз для систем Інтернет-банкінгу // Фінансовий простір. 2014. №3 (15).С. 33 – 38.
14. Конев А.А. Подход к построению модели угроз защищаемой информации // Доклады ТУСУРа. Томск, 2012. № 1(25). Часть 2. С. 34 – 40.
15. Семко В.В. Модель конфлікту взаємодії об'єктів кібернетичного простору // Проблеми інформатизації та управління. 2012. Вип. 2(38). С. 88 – 92. URL: http://jrnl.nau.edu.ua/index.php/PIU/article/download/6503/7279.
16. Маслоу А. Мотивация и личность / пер. А.М. Татлыбаевой; терминолог. правка В. Данченка. К.: PSYLIB, 2004. 384 с.
17. Лефевр В.А., Смолян Г.Л. Алгебра конфликта. М.: Знание, 1968. 64 с. (Математика, кибернетика).
18. Жарков Я.М., Дзюба М.Т., Замаруєв І.В. Інформаційна безпека особистості, суспільства, держави: підручник. К.: Видавничо-поліграфічний центр «Київський університет», 2008. 274 с.
19. Козубцов І.М., Хлапонін Ю.І., Козубцова Л.М. Ідея впровадження зворотного зв'язку як вдосконалення функціональної залежності реалізації кібернетичної безпеки // Міжнародна науково-практична конференція "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку" (Харків, 15 березня 2021 р.). Харків. Національна академія Національної гвардії України, 2021. С. 86 – 87.