**Инженерный вестник Дона**, №9 (2021)
ivdon.ru/ru/magazine/archive/n9y2021/7187

# Рефлексивно управляемые кибервойны современности с позиции когнитивного моделирования

*И. В. Лапшина, Е. А. Першонкова*
*Таганрогский институт имени А. П. Чехова (филиал) РГЭУ (РИНХ)*

**Аннотация:** В работе авторами рассматривается проблема рефлексивно управляемых кибервойн современности на примере воздействия в киберпространстве, которое в настоящее время является одновременно средой для конфликта и его инструментом. Анализируются реализованные кибератаки и опасность хакерских атак. Отдельно отмечается, что риски, связанные с кибервторжениями, могут включать потерю или раскрытие потребительских данных, кражу или раскрытие интеллектуальной собственности, а также потери инвесторов в результате кражи средств или снижения рыночной стоимости компаний, подвергшихся кибератакам. Делается вывод о том, что кибербезопасность − это постоянно развивающийся ландшафт, и в настоящее время возникает острая необходимость в том, чтобы постоянно учиться как на собственном опыте, так и на опыте других компаний, эффективно противодействующих кибератакам. Кроме того, важным условием является то, что успешное взаимодействие с противниками в киберпространстве требует постоянного стремления к тактической, оперативной и стратегической инициативе.

**Ключевые слова:** кибервойны, кибератаки, риски кибербезопасности, сети связи, транспортные системы, тактическая, оперативная и стратегическая инициативы.

В начале нашего исследования мы проанализируем практику «малых» войн и вооруженных конфликтов, произошедших в мире за пределами постсоветского пространства, что вполне объяснимо, учитывая, что прошедший XX век столетие противостояний различного уровня. Центральной опасностью в мировом сообществе, на наш взгляд, стал тот факт, что Америка вошла в перманентную «глобальную войну с терроризмом», ведущуюся, по сути, по всему Земному шару в форме множества больших и малых интервенционных действий [1].

Так, ярким примером конфликта может служить конфликт между сингалами (буддистами по вероисповеданию) и тамилами (индуистами) на Шри-Ланке в 1987 г., в котором «Тигры освобождения Тамил Илама» стали прибегать к практике нападений бомбистов-самоубийц, соответственно была проведена специальная подготовка кадров фанатиков-камикадзе, что, в свою очередь, можно позиционировать как вариант начального уровня подготовки сетевого воина с точки зрения воздействия на сознание будущего смертника.

Далее скажем о вооруженном конфликте 1995 г. между двумя латиноамериканскими странами Перу и Эквадором. Преимуществом в данном вооруженном конфликте было то, что Эквадор смог организовать достаточно успешное наведение своей авиации с помощью своевременно развернутой у линии границы наземной РЛС, в то время как у перуанской стороны радиолокационное покрытие в зоне конфликта полностью отсутствовало, что можно также охарактеризовать как элемент сетецентричной войны, т.е. войны нового типа.

В настоящее время основной тактический принцип российской информационной войны – понятие «рефлексивного управления». Как пишет Timothy L. Thomas, аналитик Центра по изучению зарубежных вооруженных сил при армии США и эксперт по новейшей российской военной истории и теории, рефлексивное управление включает в себя «передачу противнику специально подготовленной информации с тем, чтобы убедить его по собственной воле принять решение, выгодное инициатору передачи» [2, с. 15]. Это позволяет фактически говорить о применении психологических принудительных механизмов, влияющих на сознание противника. «В то время как кибервойна на военном уровне относится к конфликту, связанному со знаниями, сетевая война относится к социальной борьбе, чаще всего связанной с конфликтами низкой интенсивности со стороны негосударственных субъектов, таких как террористы, наркокартели или распространители оружия массового уничтожения на черном рынке» [3].

Следовательно, будущие войны будут вестись за гражданскую и военную инфраструктуру, спутниковые системы, электрические сети, сети связи и транспортные системы, а также сети между людьми. Оба этих поля битвы – электронное и человеческое – подвержены манипулированию алгоритмами противника [4,5].

Роза Брукс − американский профессор права, журналист, автор и комментатор по внешней политике США замечает, что «…кибербитвы будут связаны с тем, кто сможет контролировать машины повседневной жизни: серверы, на которые полагаются Пентагон и Нью-Йоркская фондовая биржа, компьютеры, которые следят за работой тормозов наших автомобилей, программное обеспечение, которое запускает наши домашние компьютеры…» [6].

В настоящее время каждому пользователю сети Интернет необходимо остерегаться мошенничества с электронной почтой и фишинга. То, что кажется законным сайтом, на самом деле может быть мошенничеством. Ссылка может быть на первый взгляд от законного продавца, но в названии, например, употребляется дополнительная буква. Чтобы быть в безопасности, необходимо заходить прямо на сайт компании, от которой пришло письмо на электронную почту, таким образом можно избежать переходов по вредоносным ссылкам, которые способны привести к случайной загрузке вредоносных или шпионских программ на компьютер, планшет или мобильный телефон.

Итак, речь идет о возможности воздействия в киберпространстве, которое является одновременно средой для конфликта и его инструментом, и здесь возникает вопрос власти и принуждения. Если классическая геополитика использует понятия Морского могущества (Sea Power) и Сухопутного могущества (Land Power), а позже появилось господство в воздухе и господство в космосе, то с недавнего времени заговорили и о новом могуществе или господстве в киберпространстве (Cyber Power). Существенной разницей между горячими войнами и потенциальными кибервойнами является, то что кибератаки пока еще не привели к гибели или увечью людей, следовательно, их нельзя классифицировать как военные действия ввиду отсутствия физического насилия [7,8].

По мнению Джозефа С. Ная «Кибермогущество может использоваться для получения предпочтительных результатов в киберпространстве, или оно может использовать киберинструменты для получения предпочтительных результатов в других областях вне киберпространства» [9]. При этом нужно отметить следующее: свобода действий – это характеристика превосходства в киберпространстве, так, например, предположительно не будут применять кибератаки против исключительно гражданских объектов. Однако это не совсем так, как показывает социальная практика. Бартон Геллман и Лаура Пойтрас в статье «British intelligence mining data from nine U.S. Internet companies in broad secret program» утверждают, что Агентство национальной безопасности и ФБР подключаются непосредственно к центральным серверам девяти ведущих американских интернет-компаний, извлекая аудио- и видеочаты, фотографии, электронную почту, документы и журналы соединений, которые позволяют аналитикам отслеживать иностранные цели, согласно сверхсекретному документу, полученному The Washington Post. Также Агентство национальной безопасности США тайно взломало основные каналы связи, соединяющие центры обработки данных Yahoo и Google по всему миру, согласно документам, полученным от бывшего сотрудника АНБ Эдварда Сноудена и интервью со знающими чиновниками [10]. В свою очередь государственные запросы на получение данных о клиентах предоставляет корпорация Microsoft и осуществляет эту деятельность, используя современные облачные технологии на основе открытости и доступности. Сотрудники Microsoft утверждают, что уделяют большое внимание уважению и защите частной жизни клиентов, однако Microsoft признает, что правоохранительные органы играют критически важную роль в обеспечении безопасности клиентов. «В то же время мы считаем, что наши клиенты заслуживают предсказуемости в том, как и когда правительство может получить доступ к их данным, и это должно зависеть от

национальных законов и международных стандартов в области прав человека, а не от усмотрения какой-либо компании, чтобы определить, где проходит граница» [11,12]. Приведем пример реализованной кибератаки Stuxnet (червь) на иранскую атомную станцию. Это было первое зарегистрированное цифровое оружие, которое использовалось для разрушения физических ресурсов. Как и любая другая атака, Stuxnet следовал ранее описанным этапам и пребывал в сети объекта в течение года. Первоначально Stuxnet использовался для манипулирования клапанами в ядерной установке, что приводило к повышению давления и повреждению нескольких устройств на станции. Затем вредоносная программа была модифицирована для атаки на более крупную цель – центрифуги. Итак, как замечают исследователи Диогенес Ю. и Озкайя Э. в работе «Кибербезопасность: стратегии атак и обороны» у иранского ядерного объекта не было никаких шансов защитить себя, поскольку злоумышленники уже получили доступ, повысили свои привилегии и остались вне поля зрения средств безопасности. Еще одним примером в современном киберпространстве является вариант манипулирования данными. Обусловлено это тем, что это уже следующая стадия киберпреступления, и ожидается, что в ближайшем будущем будет еще много таких случаев. Говорят, что промышленные предприятия США не готовы к таким атакам. Эксперты по кибербезопасности предупреждают о неминуемых угрозах манипуляционных атак на медицинские, финансовые и правительственные данные [13, с. 96]. Велика в настоящее время опасность хакерских атак, и в данном случае сочетание вседозволенности с невидимостью делает хакеров опасными. Кибербезопасность стала важной темой как в частном, так и в государственном секторах, и не без оснований. Правоохранительные органы и финансовые регуляторы публично заявляют, что кибератаки становятся все более частыми и изощренными.

Киберугрозы продолжают приобретать все большее значение для учреждений финансовых услуг и других компаний, которые стали мишенью для изощренных хакерских групп. Они могут спокойно перехватывать в сети пароли и данные, добавлять в программы закладки для последующего несанкционированного доступа и атаковать другие узлы сети. Как отмечает Эриксон Д. Хакинг, вирусы и черви становятся причиной многочисленных неприятностей и приносят бизнесу большие убытки, но в то же время они заставляют разработчиков принимать ответные меры для решения возникших проблем. Черви самовоспроизводятся, используя уязвимости некачественного программного обеспечения. Зачастую ошибки остаются незамеченными на протяжении лет, а относительно безвредные черви, такие, как CodeRed или Sasser, заставляют разработчиков их исправить» [14, с. 350]. Предприятия, таким образом, должны проводить регулярные комплексные оценки рисков угроз кибербезопасности, с которыми они сталкиваются, включая внешние и внутренние угрозы и уязвимости своих активов. Хотя в настоящее время не существует «единого для всех» варианта достойным образом подготовиться к различным способам кибератаки и к тому, какие ответные меры могут быть уместны, плохо реализованный ответ на киберсобытие может быть столь же разрушительным. Как отмечают аналитики, недостаточно продуманный ответ может быть гораздо более разрушительным, чем сама атака. Соответственно, предприятия должны тратить время и ресурсы на то, чтобы убедиться, что их руководство разработало хорошо продуманный план реагирования, который соответствует лучшим практикам для компании в той же отрасли.

Иными словами, прежде чем киберриски могут быть нейтрализованы, команда по обеспечению безопасности должна провести углубленный анализ уязвимостей, с которыми она сталкивается. В идеальной IT среде команда по обеспечению безопасности может реагировать на все уязвимости, поскольку

у нее достаточно ресурсов и времени. Однако в действительности существует очень много ограничивающих факторов, когда речь идет о ресурсах, доступных для нейтрализации рисков. Вот почему оценка рисков имеет решающее значение.

Так, если риски кибербезопасности существенно влияют на продукты, услуги, отношения организации с клиентами или поставщиками или конкурентные условия, организация должна раскрывать такие риски. Риски кибербезопасности и инциденты, которые представляют собой существенные затраты на предотвращение или реагирование, должны быть преданы гласности [15].

Все это позволяет исследователям говорить о том, что кибератака может не иметь прямого материального негативного воздействия на саму компанию, но потеря персональных и финансовых данных клиентов может иметь разрушительные последствия для жизни самих клиентов компании. В таких случаях правильно будет дать этим жертвам предупреждение, чтобы они могли защитить себя. Кроме вышеотмеченного, надо сказать и о следующем аспекте, связанным с широким диапазоном проблем, направленных на решение задач по обеспечению кибербезопасности предприятиями. Вот, например, Алан Вудворд, эксперт по кибербезопасности и профессор Университета Суррея (Англия), отмечает, что сосредоточение внимания на обучении людей нетехническим ролям, чтобы они были более подготовленными в области обеспечения безопасности в киберпространстве, как правило, накладывает слишком большую нагрузку на людей [16]. Кибербезопасность это постоянно развивающийся ландшафт, и сегодня возникает острая необходимость в том, чтобы постоянно учиться как на собственном опыте, так и на опыте других.

В настоящее время мир и международные отношения в нем характеризуются многими существенными процессами, которые только лишь

начинают подвергаться исследованиям специалистов в области общественных наук. В целом, эксперты склоняются к мнению, что само основание кибервойск увеличивает способность вооруженных сил действовать в киберпространстве, киберзащита требует «защиты вперед», участие в реальных международных военных операциях будет ценным с позиции приобретения навыков развития киберинструментов и в целом кибервойск.

В международных отношениях сферу киберпространства уже нельзя считать чем-то второстепенным, поскольку в современных боевых операциях киберинструменты считаются жизненно необходимыми для успешного выполнения многочисленных задач. Деятельность в киберпространстве со временем может подорвать источники национальной мощи страны. Возникает острая необходимость в том, чтобы правительственные сети и оборонная промышленность государств стали обладать все возрастающей киберспособностью, поскольку из области открытого конфликта и насильственных операций сфера противостояния переходит в киберпространство, минуя сферу военных конфликтов с применением летального оружия. Усилия в области кибербезопасности должны включать, помимо оценки, предотвращение и смягчение последствий, устойчивость и восстановление.

В современных условиях кибератаки совершаются похитителями личных данных, недобросовестными подрядчиками и поставщиками, злонамеренными сотрудниками, конкурентами по бизнесу, потенциальными инсайдерскими трейдерами и рыночными манипуляторами, так называемыми «хактивистами», террористами, спонсируемыми государством субъектами и другими. Киберпреступления могут создавать значительные риски для операционной деятельности участников рынка и рынков в целом. Эти риски могут принимать форму отказа в обслуживании и разрушения систем,

потенциально приводя к препятствиям для доступа к счету и выполнения транзакций, а также нарушению других важных функций рыночной системы. Риски, связанные с кибервторжениями, могут также включать потерю или раскрытие потребительских данных, кражу или раскрытие интеллектуальной собственности, а также потери инвесторов в результате кражи средств или снижения рыночной стоимости компаний, подвергшихся кибератакам. Участники рынка также сталкиваются с регуляторными, репутационными и судебными рисками, возникающими в результате киберинцидентов, а также с потенциальными значительными затратами на исправление ситуации.

Samuel P. Huntington выделяет два важнейших фактора, определяющих успех стратегической концепции: ресурсы, как человеческие, так и материальные, необходимые для ее реализации, и организационная структура, которая группирует ресурсы, выделяемые обществом таким образом, чтобы реализовать стратегическую концепцию [17].

Состав блоков и их взаимодействие в модели «Рефлексивно управляемые кибервойны современности» (См. рис.1). Модель **«Киберпространство с позиции взаимодействия в поле киберинцидентов»**

Состав блоков: кибервойна на военном уровне − это конфликт, кибербитвы будут связаны с тем, кто сможет контролировать машины повседневной жизни, фишинг в сети Интернет, господство в киберпространстве, взлом основных каналов связи, соединяющие центры обработки данных Yahoo и Google, Microsoft признает, что правоохранительные органы играют критически важную роль в обеспечении безопасности клиентов, кибератака Stuxnet на иранскую атомную станцию − вне поля зрения средств безопасности, в современном киберпространстве осуществляется манипулирование данными (медицинские, финансовые и правительственные), правоохранительные органы и финансовые регуляторы

публично заявляют, что кибератаки становятся все более частыми и изощренными.

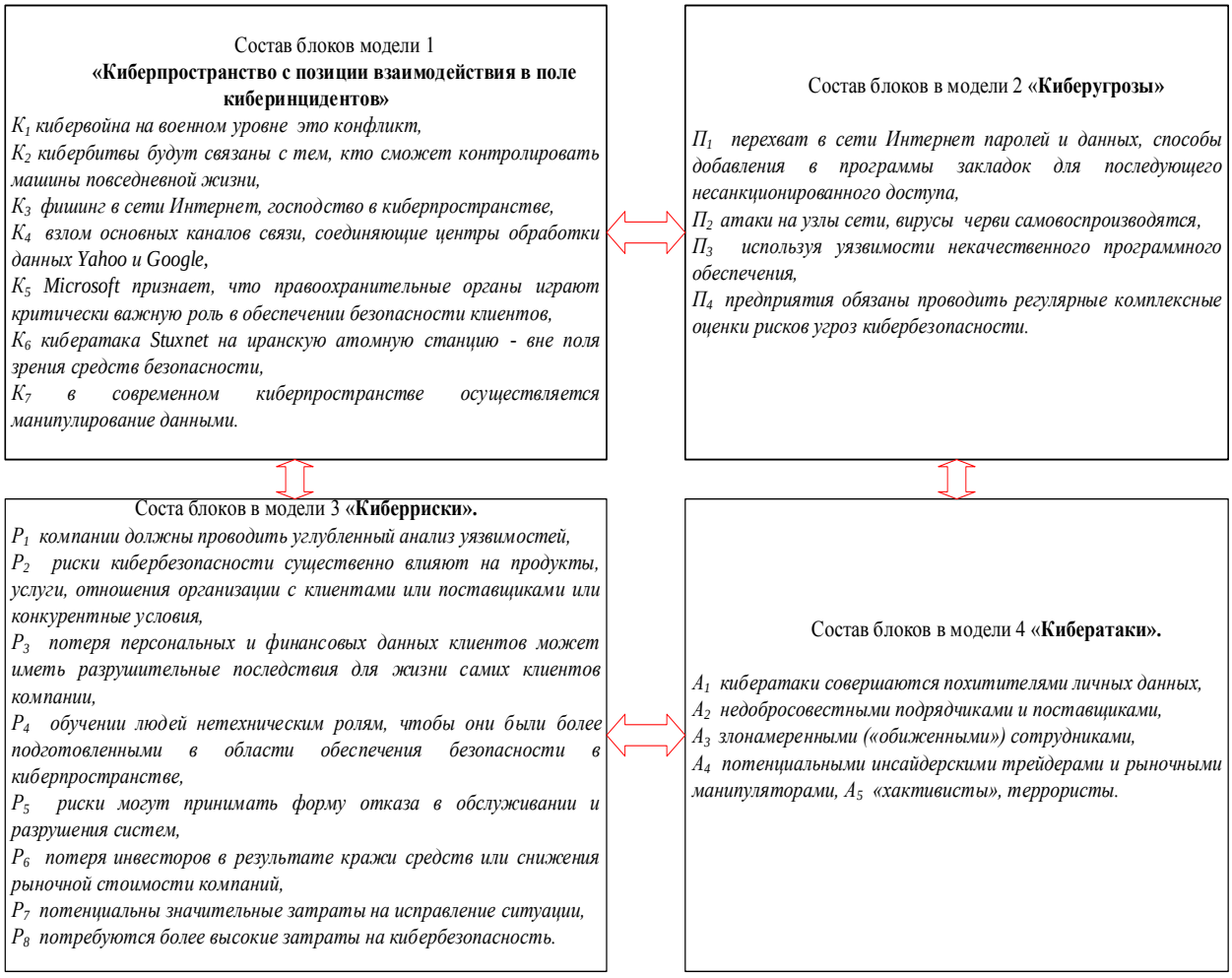


Рис. 1. – Состав и взаимодействие блоков модели «Рефлексивно управляемые кибервойны современности»

Состав и взаимодействие блоков модели: «**Киберугрозы».**

Состав блоков: перехват в сети Интернет паролей и данных, способы добавления в программы закладок для последующего несанкционированного доступа, атаки на узлы сети, вирусы черви самовоспроизводятся, используя уязвимости некачественного программного обеспечения, предприятия обязаны проводить регулярные комплексные оценки рисков угроз кибербезопасности.

Состав и взаимодействие блоков модели: «**Киберриски».**

Состав блоков: компании должны проводить углубленный анализ уязвимостей, риски кибербезопасности существенно влияют на продукты, услуги, отношения организации с клиентами или поставщиками или конкурентные условия, потеря персональных и финансовых данных клиентов может иметь разрушительные последствия для жизни самих клиентов компании, обучение людей нетехническим ролям, чтобы они были более подготовленными в области обеспечения безопасности в киберпространстве, риски могут принимать форму отказа в обслуживании и разрушения систем, потеря инвесторов в результате кражи средств или снижения рыночной стоимости компаний, потенциальны значительные затраты на исправление ситуации, потребуются более высокие затраты на кибербезопасность.

Состав и взаимодействие блоков модели: «**Кибератаки».**

Состав блоков: кибератаки совершаются похитителями личных данных, недобросовестными подрядчиками и поставщиками, злонамеренными («обиженными») сотрудниками, потенциальными инсайдерскими трейдерами и рыночными манипуляторами, «хактивистами», террористами.

Выделим блоки факторов в модели 1 **«Киберпространство с позиции взаимодействия в поле киберинцидентов»**

$К_1$ – кибервойна на военном уровне – это конфликт, $К_2$ – кибербитвы будут связаны с тем, кто сможет контролировать машины повседневной жизни, $К_3$ – фишинг в сети Интернет, господство в киберпространстве, $К_4$ – взлом основных каналов связи, соединяющие центры обработки данных Yahoo и Google, $К_5$ – Microsoft признает, что правоохранительные органы играют критически важную роль в обеспечении безопасности клиентов, $К_6$ – кибератака Stuxnet на иранскую атомную станцию − вне поля зрения средств безопасности, $К_7$ – в современном киберпространстве осуществляется манипулирование данными.

Выделим блоки факторов в модели 2 «**Киберугрозы».**

$П_1$ – перехват в сети Интернет паролей и данных, способы добавления в программы закладок для последующего несанкционированного доступа, $П_2$ – атаки на узлы сети, вирусы – черви самовоспроизводятся, $П_3$ – используя уязвимости некачественного программного обеспечения, $П_4$ – предприятия обязаны проводить регулярные комплексные оценки рисков угроз кибербезопасности.

Выделим блоки факторов в модели 3 «**Киберриски».**

$Р_1$ – компании должны проводить углубленный анализ уязвимостей, $Р_2$ – риски кибербезопасности существенно влияют на продукты, услуги, отношения организации с клиентами или поставщиками или конкурентные условия, $Р_3$ – потеря персональных и финансовых данных клиентов может иметь разрушительные последствия для жизни самих клиентов компании, $Р_4$ – обучение людей нетехническим ролям, чтобы они были более подготовленными в области обеспечения безопасности в киберпространстве, $Р_5$ – риски могут принимать форму отказа в обслуживании и разрушения систем, $Р_6$ – потеря инвесторов в результате кражи средств или снижения рыночной стоимости компаний, $Р_7$ – потенциальны значительные затраты на исправление ситуации, $Р_8$ – потребуются более высокие затраты на кибербезопасность.

Выделим блоки факторов в модели 4 «**Кибератаки».**

$А_1$ кибератаки совершаются похитителями личных данных, $А_2$ недобросовестными подрядчиками и поставщиками, $А_3$ злонамеренными («обиженными») сотрудниками, $А_4$ потенциальными инсайдерскими трейдерами и рыночными манипуляторами, $А_5$ «хактивисты», террористы.

Известно, что когнитивная карта представляет собой взвешенный ориентированный граф [18-20].

$$G = <V, E>,$$

где V – вершины графа:

$$V = \{v_i\}, v \in V, i = \overline{1,k};$$

E – дуги графа: (1)

$$E = \{e_i\}, e \in E, i = \overline{1,k}.$$

На рис. 1-4 сплошные линии и символ «+1,00» обозначают положительную связь между вершинами *Vi* и *Vj*, то есть увеличение (уменьшение) влияния вершины *Vi* вызывает увеличение (уменьшение) в вершине *Vj*, линии и символ «–1,00» означают отрицательную связь между *Vi* и *Vj*, то есть увеличение (уменьшение) влияния вершины *Vi* вызывает уменьшение (увеличение) в вершине *Vj* [См. 1].

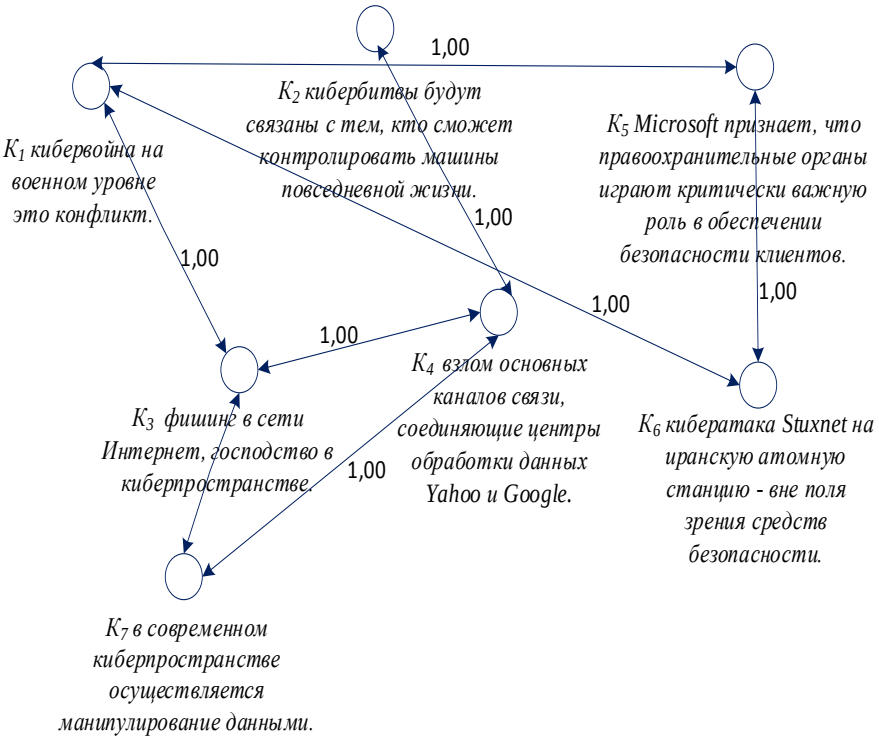


Рис. 2. − Взаимодействие блоков в модели 1 «Киберпространство с позиции взаимодействия в поле киберинцидентов»

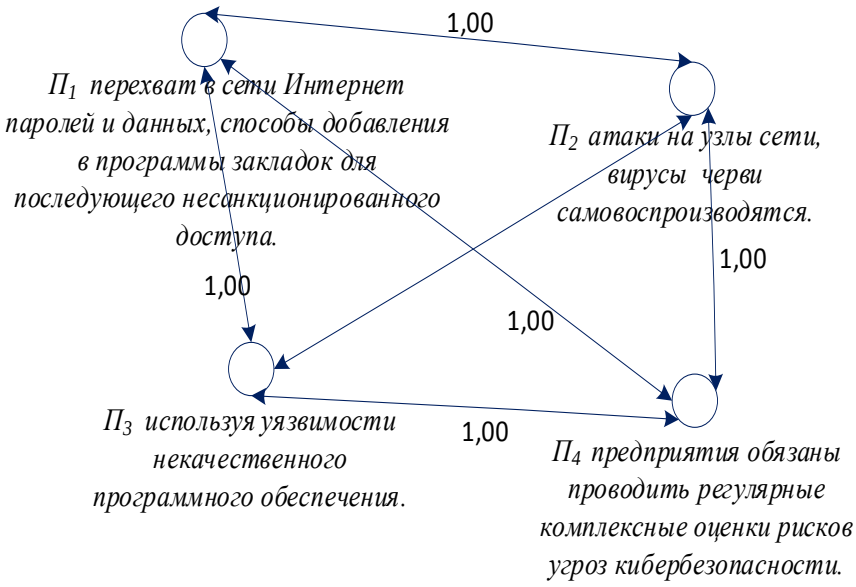


Рис. 3. − Взаимодействие блоков в модели 2 «Киберугрозы»

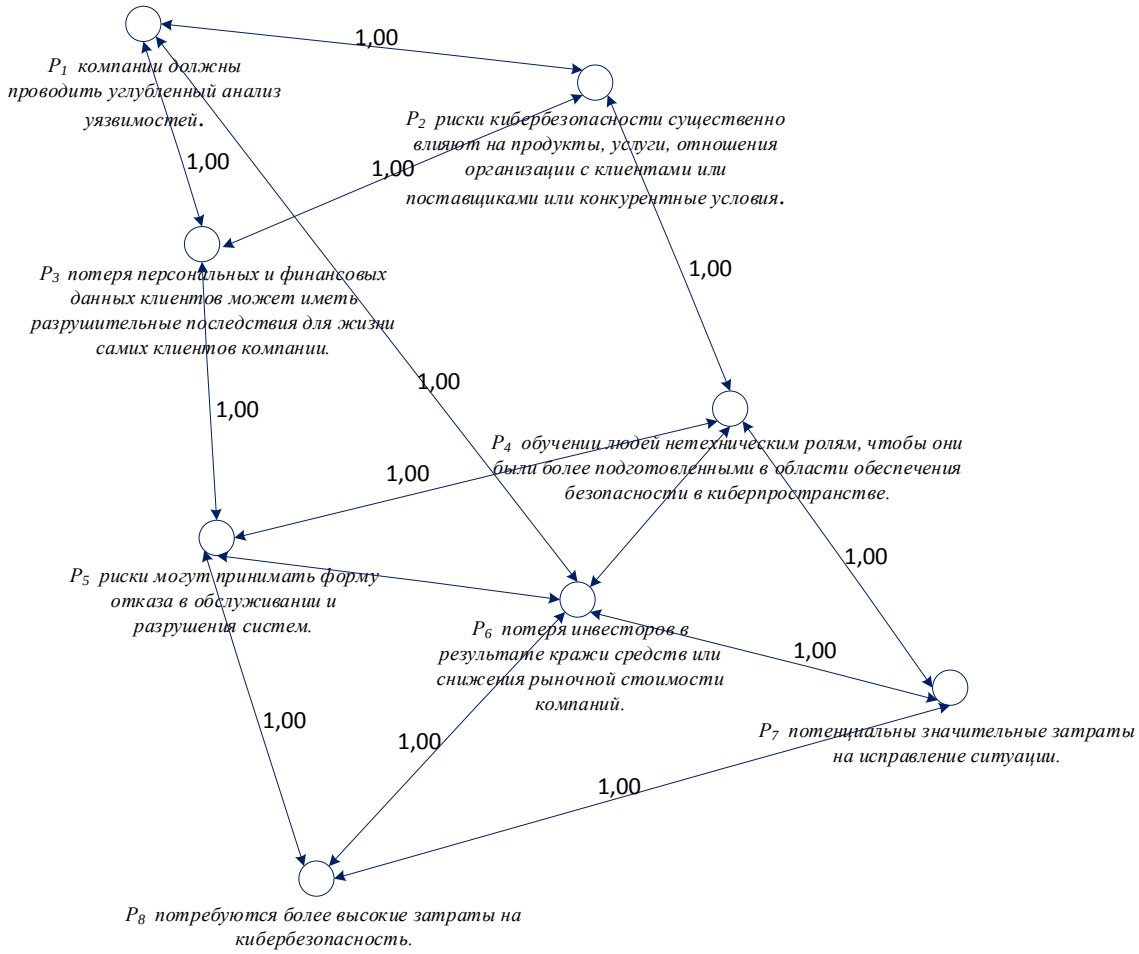


Рис. 4. − Взаимодействие блоков в модели 3 «Киберриски»

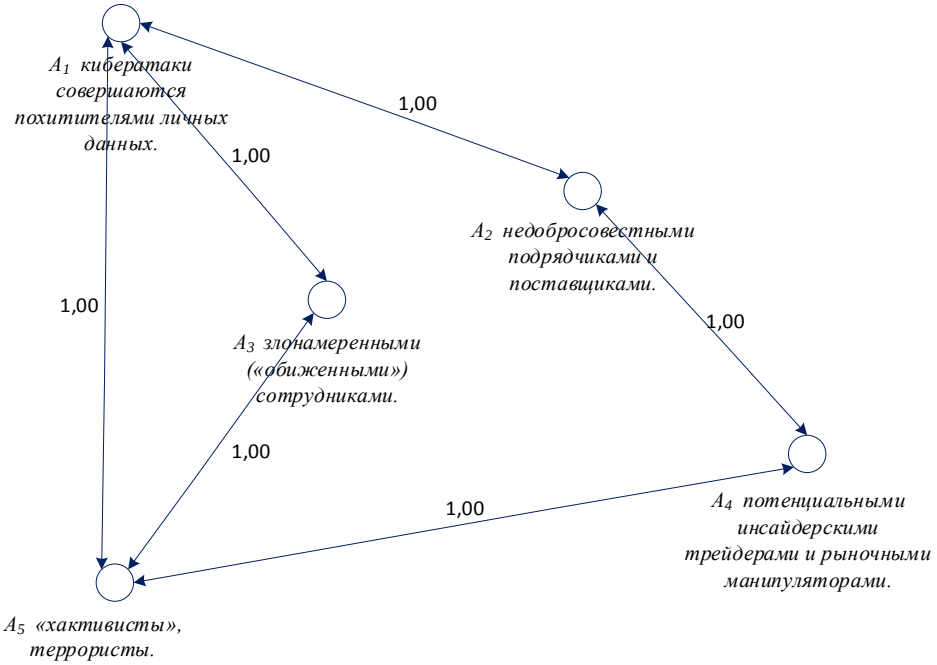


Рис. 5. − Взаимодействие блоков в модели 4 «Кибератаки»

Итак, на рис. 1 – 5 представлены когнитивные карты, которые наглядно демонстрируют взаимосвязь блоков, полученных в ходе проведенного анализа социальных практик, связанных с проведением потенциальных рефлексивно управляемых кибервойн.

В ходе проведения когнитивного моделирования мы построили когнитивную карту «Рефлексивно управляемых кибервойны современности» и выявили дополнительные связи блоков, имеющих взаимное влияние друг на друга: К2+П4, К3+А1, К4+А5, К7+П3, К7+Р5, Р4+А4, Р8+П1, К7+П3, К6+П3, А2+П4, А1+П3, Р7+А1 (См. рис. 6)

Таким образом, повышенный акцент на кибербезопасность для всех компаний, ориентированных на получение, обработку и хранение данных, приведет к тому, что потребуются более высокие затраты на кибербезопасность, что в свою очередь приведет к нанесению вреда прибыли компании с позиции ее понижения и может помешать свободному денежному потоку в обозримом будущем. Здесь же стоит отметить, что

кибератаки в настоящее время сосредоточены не только на краже данных, но и на их изменении без обнаружения.

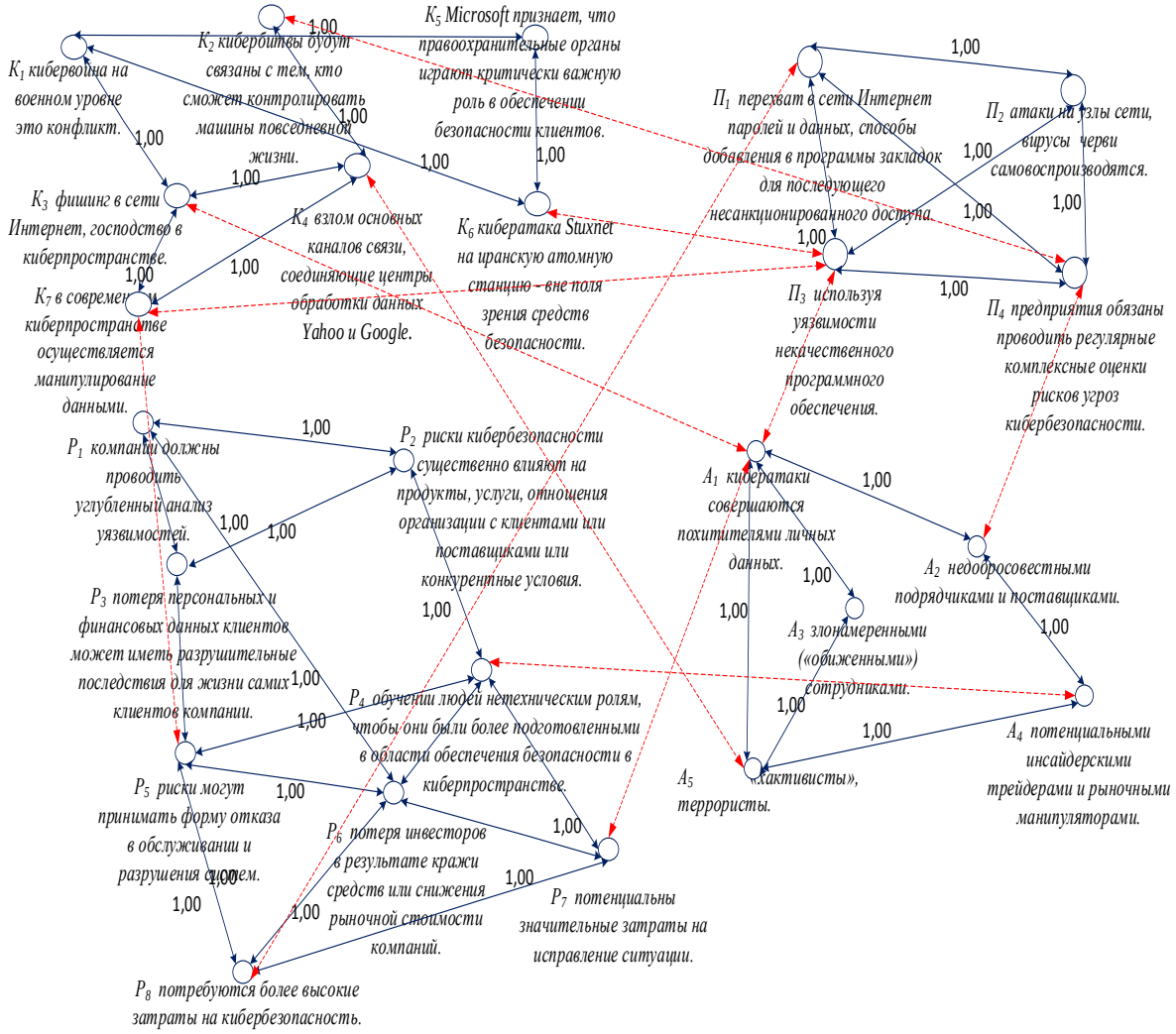


Рис. 6. − Когнитивная карта модели «Рефлексивно управляемые кибервойны современности»

Более того, успешное взаимодействие с противниками в киберпространстве требует постоянного стремления к тактической, оперативной и стратегической инициативе. Также надо отметить и то, что определение национального протокола кибербезопасности должно быть главным приоритетом в вопросах, связанных с обеспечением национальной безопасности государства.

**Литература**

1. Барабанов М., Коновалов И., Куделев В., Целуйко В. Чужие войны // под ред. Пухова Рю // ЛитВек. Время электронных книг. URL: litvek.com/book-read/253226-kniga-mihail-sergeevich-barabanov-chuzhie-voynyi-chitat-online?p=1.

2. Кемаль А. Кибервойна. Как Россия манипулирует миром. 2015. // Bookash.pro. URL: bookash.pro/ru/book/47536/kibervoina-kak-rossiya-manipuliruet-mirom-andrei-kemal.

3. Савин Л. В. Стрелы кентавра. Кибервойна по-американски. Издательский дом «Кислород», 2020. // ЛитМир. Электронная библиотека. URL: litmir.me/br/?b=688013&p=1.

4. Pernik P. Preparing for Cyber Conflict: Case Studies of Cyber Command. Tallinn: International Centre for Defence and Security, December, 2018.

5. Weinbaum, Cortney and Shanahan, John N.T. Intelligence in a Data-Driven Age // Joint Force Quarterly. 2018. Vol. 90, 3rd Quarter. p. 4-9.

6. Brooks R. How Everything Became War and the Military Became Everything: Tales from the Pentagon. Simon Schuster, 2016. p. 448.

7. Thomas R. Think Again: Cyberwar // Foreign Policy. 2012. February 27. URL: foreignpolicy.com/articles/2012/02/27/cyberwar#6.

8. Kissinger Henry. World Order. Penguin Books Limited, 2014. p.196.

9. Nye Joseph S. Jr. The Future of Power. New York: Public Affairs, 2011. p. 123.

10. British intelligence mining data from nine U.S. Internet companies in broad secret program // The Washington Post. 2013. June 7. URL: washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

11. Barton Gellman and Ashkan Soltani, NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say // The Washington Post. 2013. October 30. URL: washingtonpost.com/world/national-security/nsa-infiltrates-linksto-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/.

12. Отчет о запросах правоохранительных органов. Запросы по странам/регионам // Microsoft. URL: microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report.

13. Диогенес Ю., Озкайя Э. Кибербезопасность: стратегии атак и обороны / пер. с анг. Д. А. Беликова. М.: ДМК Пресс, 2020. 326 с.

14. Эриксон Д. Хакинг: искусство эксплойта. 2-е изд. СПб.: Питер, 2018. 496 с.

15. U.S. Department of the Treasury URL: treasury.gov/press-center/Video-Audio-Webcasts/Pages/Webcasts.aspx.

16. Keane Jonathan. Training staff to be wary of a cyber threat is not a clear-cut job. // CNBC. 2021. June 28. URL: cnbc.com/2021/06/28/training-staff-to-be-wary-of-a-cyber-threat-is-not-a-clear-cut-job.html?&qsearchterm=cyber.

17. Huntington Samuel P. National Policyand the Transoceanic Navy // U.S. Naval Institute Proceedings. 1954. Vol. 90, № 5 (May) p. 483-493.

18. Максимов В. И. Структурно-целевой анализ развития социально-экономических ситуаций: автореф. дис. ... д-р техн. наук: 05.13.10. М., 2002. 54 с.

19. Лапшина И. В., Калугина Л. И. Сравнительный анализ конфликтогенности советского и современного молодежного пространства с использованием когнитивного моделирования // Инженерный вестник Дона, 2019, №6 URL: ivdon.ru/ru/magazine/archive/n6y2019/6018.

20. Гинис Л. А., Давыденко О. В. Применение когнитивного теоретико-множественного подхода к задаче определения кадастровой

стоимости земель. // Инженерный вестник Дона, 2019, №7 URL: ivdon.ru/ru/magazine/archive/n7y2019/6110.

**References**

1. Barabanov M., Konovalov I., Kudelev V., Tseluyko V. Chuzhiye voyny [Other people's Wars]. Pod red. R. Pukhova. LitVek. Vremya elektronnykh knig. URL: litvek.com/book-read/253226-kniga-mihail-sergeevich-barabanov-chuzhie-voynyi-chitat-online?p=1.

2. Kemal′ A. Kibervoyna. Kak Rossiya manipuliruyet mirom [How Russia manipulates the world]. 2015. Bookash.pro. URL: bookash.pro/ru/book/47536/kibervoina-kak-rossiya-manipuliruet-mirom-andrei-kemal.

3. Savin L. V. Strely kentavra. Kibervoyna po-amerikanski [Centaur arrows. Cyberwar in the American way]. Izdatel′skiy dom «Kislorod», 2020. LitMir. Elektronnaya biblioteka. URL: litmir.me/br/?b=688013&p=1.

4. Pernik P. Preparing for Cyber Conflict: Case Studies of Cyber Command. Tallinn: International Centre for Defence and Security, December, 2018.

5. Weinbaum, Cortney and Shanahan, John N.T. Intelligence in a Data-Driven Age. Joint Force Quarterly. 2018. Vol. 90, 3rd Quarter. p. p. 4-9.

6. Brooks R. How Everything Became War and the Military Became Everything: Tales from the Pentagon. Simon Schuster, 2016. p. 448.

7. Thomas R. Think Again: Cyberwar. Foreign Policy. 2012. February 27. URL: foreignpolicy.com/articles/2012/02/27/cyberwar#6.

8. Kissinger Henry. World Order. Penguin Books Limited, 2014. p.196.

9. Nye Joseph S. Jr. The Future of Power. New York: Public Affairs, 2011. p. 123.

10. British intelligence mining data from nine U.S. Internet companies in broad secret program. The Washington Post. 2013. June 7. URL:

washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secretprogram/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

11. Barton Gellman and Ashkan Soltani, NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say. The Washington Post. 2013. October 30. URL: washingtonpost.com/world/national-security/nsa-infiltrates-linksto-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/.

12. Otchet o zaprosakh pravookhranitel′nykh organov. Zaprosy po stranam/regionam [Report on requests from law enforcement agencies. Queries by country/region]. Microsoft. URL: microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report.

13. Diogenes YU., Ozkayya E. Kiberbezopasnost′: strategii atak i oborony [Cybersecurity: Attack and defense strategies]. Per. s ang. D. A. Belikova. M.: DMK Press, 2020. 326 p.

14. Erikson D. Khaking: iskusstvo eksployta [Hacking: the art of the exploit]. 2-e izd. SPb.: Piter, 2018. 496 p.

15. U.S. Department of the Treasury URL: treasury.gov/press-center/Video-Audio-Webcasts/Pages/Webcasts.aspx.

16. Keane Jonathan. Training staff to be wary of a cyber threat is not a clear-cut job. CNBC. 2021. June 28. URL: cnbc.com/2021/06/28/training-staff-to-be-wary-of-a-cyber-threat-is-not-a-clear-cut-job.html?&qsearchterm=cyber.

17. Huntington Samuel P. National Policyand the Transoceanic Navy. U.S. Naval Institute Proceedings. 1954. Vol. 90, № 5 (May). p. 483-493.

18. Maksimov V. I. Strukturno-tselevoy analiz razvitiya sotsial′no-ekonomicheskikh situatsiy [Structural and target analysis of the development of socio-economic situations]: avtoref. dis. ... d-r tekhn. nauk: 05.13.10. M., 2002. 54 p.

19. Lapshina I. V., Kalugina L. I. Inzhenernyj vestnik Dona, 2019, № 6. URL: ivdon.ru/ru/magazine/archive/n6y2019/6018.

20. Ginis L. A., Davydenko O. V. Inzhenernyj vestnik Dona, 2019, № 7. URL: ivdon.ru/ru/magazine/archive/n7y2019/6110.