DOI: 10.18372/2410-7840.20.13422
УДК 004.056

ПРЕДПОСЫЛКИ ДЛЯ ФОРМИРОВАНИЯ БЕЗОПАСНОЙ ИНФОРМАЦИОННО-ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ СОВРЕМЕННОГО УНИВЕРСИТЕТА

Лазат Кыдыралина

В работе проведен обзор и анализ предшествующих исследований в сфере обеспечения защиты информационно-образовательной среды университетов (ИОСУ). Показано, что приоритетность развития цифровых систем образования во многих промышленно развитых государствах мира требует соответствующей технико-методологической поддержки специалистов не только в области педагогической деятельности, но и информационных технологий с учетом проблематики кибербезопасности и защиты информации. Показано, что к защищаемым сведениям, которые хранятся и циркулируют в информационно-коммуникационных системах университетов, в частности относятся: персональные данные учащихся, преподавателей, научных сотрудников, вспомогательного персонала; оцифрованная информация, представляющая интеллектуальную собственность учебного заведения; информационные массивы, которые, обеспечивают учебный процесс, (например, мультимедийный контент, базы данных, обучающие программы); др. Обосновано, что данные информационные ресурсы могут выступить как объект хищения или искажения со стороны внешних (внутренних) компьютерных злоумышленников или из хулиганских побуждений, со стороны учащихся или сотрудников.Обосновано, что сформированный во многих странах тренд на глобализацию доступа к информационным ресурсам делает релевантными задачи внедрения новейших цифровых и информационно-коммуникационных технологий во все сферы деятельности современного вуза. Обоснована актуальность исследований в направлении разработки моделей для систем поддержки решений по нахождению стратегий управления инвестированием для различных соотношений параметров инвестиционного процесса в системы кибербезопасности образовательных учреждений.

Ключевые слова: *кибербезопасность, информационно-образовательная среда университета, многошаговая игра качества, оптимальные стратегии финансирования.*

Введение. Приоритетность развития цифровых систем образования во многих промышленно развитых государствах мира потребовала и соответствующей технико-методологической поддержки специалистов не только в области педагогической деятельности, но и ИТ. Таким образом сформированный во многих странах тренд на глобализацию доступа к информационным ресурсам делает релевантными задачи внедрения новейших цифровых и информационно-коммуникационных технологий во все сферы деятельности современного вуза [1, 2].

Еще в конце прошлого века, но особенно активно в начале 21-гока стал применяться термин - информационная образовательная среда вуза [3]. Это понятие во многих научных публикациях [3-7] трактуется: «Как совокупность компьютерных средств и способов их функционирования, которые используются для реализации обучающей деятельности» [6, 7]. Многие аспекты создания ИОСУ уже были достаточно подробно исследованы в работах таких авторов как Г.В. Абрамян, И.Г. Захарова, Г.П. Путилов и ряда других. В Казахстане подобными исследованиями занимались С.А. Абдыманапов, Б.С. Ахметов, Р.М. Джумагалиев, В.В. Яворский и другие. Однако за рамками большинства существующих исследований, посвященных проблематике развития ИОС университетов остались аспекты, связанные с задачами обеспечения защиты информации и кибербезопасности информационно-коммуникационных систем университетов от любых видов деструктивного вмешательства со стороны компьютерных злоумышленников [8-11].

Глобализация образования вывела вопросы использования информационных технологий и систем в (ИТС) университетах на первое место. Однако при этом не всегда уделялось внимание параллельному рассмотрению задач обеспечения информационной и кибербезопасности (далее, соответственно ИБ и КрБ) как сотрудников, так и учащихся.

Специалистами в области ИТ не раз отмечалось [11], что в задачах поддержки ИБ и КрБ ресурсное обеспечение и управление защитными механизмами вузов (в равной степени и других учебных заведений, или образовательных учреждений (ОУ)) требует решения ряда проблем: необходимость устранения недостаточной оснащенности техническими средствами защиты информации (ТРЗИ); отсутствие профильной подготовки у персонала, отвечающего за ИБ и КрБ

университета; оптимизация в задачах распределения целевого финансирования на ИБ и КрБ вуза; и другое.

Современные учебные заведения объединяют в своих стенах большое количество высококвалифицированных преподавателей, сотрудников научных подразделений, студентов, а также обслуживающий персонал.

Однако постоянно накапливая разнообразную информацию как учебного и методического (методологического) характера, так и другие данные, например, касающиеся процессов в ОУ, личных данных сотрудников и студентов, ИТ специалисты университетов столкнулись с дополнительными проблемами. Прежде всего, отметим отсутствие четкой процедуры в аккумулировании и практическомприменении разрозненных и разно форматных информационных ресурсов. При этом данные ресурсы часто не проходят процедур аудита на предмет их ИБ и КрБ. Многие из программных продуктов, инсталлированных в информационно-образовательной среде университета (ИОСУ) между собой никак не связаны, часто получены из недостоверных или скомпрометированных источников, следовательно, могут представлять потенциальную опасность для ИОСУ.

Отметим, что к защищаемым сведениям, которые хранятся и циркулируют в информационно-коммуникационных системах университетов (ИКСУ) можно отнести [2, 4, 7]: персональные данные учащихся, преподавателей, научных сотрудников, вспомогательного персонала; оцифрованная информация, представляющая интеллектуальную собственность учебного заведения; информационные массивы, которые, обеспечивают учебный процесс, (например, мультимедийный контент, базы данных, обучающие программы); др.

Эта информация может выступить как объект хищения или искажения со стороны внешних (внутренних) компьютерных злоумышленников (КЗЛ) или из хулиганских побуждений, со стороны учащихся или сотрудников.

В процессе диссертационного исследования был выполнен анализ по результатам аудита ИБ и КрБмеждународных компаний, занимающихся соответствующей проблематикой для государственных организаций, в том числе для университетов и других крупных образовательных учреждений (ОУ). В первую очередь речь идет о государствах ЕС, США и Канаде [10, 11]. Как показали результаты подобных исследований [9, 11], а также данныеприведенные в работах [12, 13], и не учитывая специфические целевые атаки направленные на переполнение буфера и нарушение криптографических протоколов [14], достаточно весомая доля нарушений связана с неавторизированным изменением данных в ИОСУ (>12 %), обходом политики ограничений на ИБ в ИОСУ (>15 %), недостаточной защитой процедуры аутентификации и др.

Цель исследования. Провести обзор и анализ предшествующих исследований в сфере обеспечения защиты информационно-образовательной среды университетов (ИОСУ) и обосновать необходимость исследований в направлении разработки моделей для систем поддержки решений по нахождению стратегий управления инвестированием для различных соотношений параметров инвестиционного процесса в системы кибербезопасности образовательных учреждений.

Обзор предшествующих исследований. В публикациях, посвященных проблематике оценивания защищенности ИОСУ [9, 14, 15] отмечается, что кроме технических задач по защите информации, циркулирующей в ИКСУ, необходимо периодически анализировать информационные риски и контролировать эффективности внедренных мероприятий, направленных на обеспечение ИБ и КрБ университета. Эти процедуры позволяют учесть: изменяемость требований в задачах защиты информации (например, от защиты контента до защиты персональной информации сотрудников и учащихся); потенциальную возможность появление новых киберугроз и уязвимостей в ИКСУ; понижение эффективности уже реализованных мероприятий по защите информации со временем; понижение надежности процессов обработки информации в ИОСУ по мере физического устаревания оборудования и программного обеспечения.

Активное внедрение и широкое использование в университетах и других учебных заведениях беспроводных, в том числе сенсорных сетей и технологий [16], породило новые уязвимости перед кибератаками класса – отказ в обслуживании.

Кроме того, как было показано в работах [17, 18] часто именно сенсорные узлы наименее защищены от несанкционированного доступа (НСД). При этом их ресурсы и сроки службы зависят от энергоснабжения, количества циклов включения-выключения, что в свою очередь, может стать целью для хакеров. Таким образом, атакующий может использовать подобные ограничения для получение полного контроля над сенсорным узлом

ИОСУ, например, над терминалом, через который осуществляется оплата за обучение или за другие услуги, предоставляемые в стенах университета (оплата за общежитие, услуги интернет, спортивный зал или др.). Сенсорные узлы также достаточно легко скомпрометировать, в частности прибегнув к DoS-атакам.

По мере развития и модернизации КВКС в них имплементируют модули и компоненты сторонних поставщиков, в частности, подлобные компоненты могут отвечать за ИБ КВКС. Но, если в ходе подобной модернизации не выполняется процедура предварительного тестирования их киберзащищенности, такие компоненты могут оказаться уязвимыми перед потенциальными атаками [19, 20].

Отметим также данные исследование [21, 22], в которых рассматривалась проблематика снижения сложности успешно проведенных кибератак, направленных на ИКС государственных структур. Так, в частности, отмечается, что уровень сложности успешных атак снизился с максимального значения, более чем на 87 % в 2004 году, до 46 % в 2018 году.

Описанные во многих литературных источниках подходы к решению вышеобозначенных проблем [17], в свое время позволили значительно продвинуться в их решении для коммерческих предприятий и организация. Однако ОУ с их спецификой организации доступа к информационным ресурсам, обуславливают несколько иную специфику организационно-технического управления ИБ и КрБ.

Заметим, что по-прежнему во многих ОУ (школах, колледжах, университетах, студенческих кампусах, библиотеках и др.) сохраняется традиционный подход к решению задач финансирования средств и систем защиты информации (ЗИ) и кибербезопасности (КБ) [10, 12]. Большая часть стратегий финансирования в системы КР предполагают лишь выделение финансовых средств на антивирусные программы и относительно не сложные сетевые средства защиты [12, 13]. Это очень простая финансовая стратегия по киберзащите ОУ. Даже опытные администраторы служб информационной и кибернетической безопасности не всегда оказываются готовы худшему варианту развития событий в ходе кибератак на компьютерные системы и сети ОУ [12, 13]. Стороне защиты информации необходимо переключить свое внимание на изменение традиционных подходов по финансированию средств КБ (СКБ). Например, перейдя при выборе финансовой составляющей стратегий инвестирования в КБ на политику, которая предполагает обнаружение и блокировку потенциальных взломов компьютерных систем и сетей ОУ ИКСТ [14-16].

В работах [16-20] отмечено, что сегодня международные инвестиционные проекты в сфере образования и, в частности в цифровые информационно-образовательные платформы, стали обычной практикой международного сотрудничества [22]. Подобные инвестиционные проекты на наш взгляд обязательно должны предполагать и глубокий анализ финансовых стратегий обеспечения кибербезопасности ОУ и их совместной информационно-образовательной среды. Как отмечают многие специалисты по защите информации (ЗИ), СКБ образовательных учреждений, в частности, крупных международных, государственных и частных университетов должны не только обеспечить сохранность информационных массивов и данных, в том числе конфиденциальных, но и гарантировать невозможность внешнего несанкционированного проникновения в ИОС ОУ [12-13]. Постоянный рост количества киберпреступлений в мире, лишь усиливает необходимость увеличения финансовых вложений в СКБ [14-16], в частности для ОУ.

Исследованиям выбора эффективных стратегий финансового инвестирования в СКБ, в частности для ОУ, посвящено достаточно большое количество публикаций [14-16].

Среди моделей ИБ и КрБ наиболее основательной и распространенной является модель Гордона-Лоеба (ГЛ) [23, 24]. Целью этой модели является решение задач, связанных с определением оптимального количества инвестиций в защиту информации. Ключевой момент в модели ГЛ – введение и разработка функции уязвимости, которая определяет уровень ИБ и КрБ для рассматриваемого объекта информатизации, в частности для ИОСУ. Информационный объект может иметь различные формы – список пользователей, бухгалтерская книга счетов, стратегический план развития, вебсайт и тому подобное. Повышение безопасности может происходить в направлении защиты конфиденциальности, целостности, аутентичности, безотказности, доступности авторизации пользователей и т.д.

Модель по своей структуре является статической. Следовательно, решения и результат наступают одновременно, а динамические эффекты, в том числе зависимость денег от времени, не учитывается.

Учитывая, что инвестиции в средства и методы ИБ и КрБ неэффективны при достаточно

малых и достаточно больших значениях уязвимости, авторы модели ГЛ, а также ряда работ [16, 17, 21], которые развили идеи, заложенные в модели ГЛ, отмечали следующее обстоятельство. Многие авторы полагают, что первой задачей управления разделением объектов на низкий, средний и высокий уровень уязвимости следует заниматься на предварительном этапе проектирования. Однако при этом авторы модели ГЛ [16, 23, 24], аналогичных моделей отметили ее недостатки:

1. Не существует простой процедуры определения вероятности нападения и уязвимости информационных массивов.

2. Проблематично определять потенциальные потери от нарушения безопасности периметров защиты и кибербезопасности объекта информатизации. (для себя заметим, что для ИОСУ эти периметры ИБ и КрБ пока достаточно условны).

3. Сложность реализации результатов исследования на конкретном объекте.

4. Не учтено, как злоумышленник будет менять свою стратегию при внесении дополнительных инвестиций для защиты, то есть отсутствует анализпротивостояние в динамическом режиме.

Несмотря на то, что модель ГЛ нашла широкое признание и получила свое развитие во многих работах в течение десяти лет с момента ееопубликования, большая часть поставленных вопросов до сегодняшнего дня не решена. Неоспоримым заслугой авторов модели является то, что они впервыеосновательно рассмотрели проблему и определили функцию уязвимости, является ключевым при рассмотрении противостояние в информационной сфере.

Определениеформы функции, выражает уязвимость динамической системы, является ключевой задачей при математическом моделировании информационного противостояния и этой задаче были посвящены работы многих исследователей [17, 20, 23].

Если обратиться к истории вопроса, то противостояние двух сторон впервые основательно рассмотрены специалистами фирмы RAND Corporation в конце второй мировой войны при разработке математических основ военного планирования. Моделью противостояния двух сторон, разработанной в рамках фирмы RAND, является модель Гросса [25], предназначенная для имитации тактических военных операций. Согласно этой модели, конфликтующие стороны обладают ресурсами X и Y, а результат их противостояния определяется целевой функцией, которая линейно зависит от разницы вложенных ресурсов и приводит к задаче линейного программирования. Задача Гросса, которая возникла при планировании военных операций, имеет ряд отличий от рассмотренных задач. Во-первых, целевая функция имеет дискретный характер, поскольку определяет количество единиц, прорвались через оборону или уничтожившие нападение, или оборона. Во-вторых, эти единицы в каждом эпизоде противоборства одинаковы для нападенияи, соответственно, для обороны.

Однотипность объектов существенно упрощает решение задачи, однако ограничивает условия противоборства. Однако, основной недостаток модели Гросса - кусочно-линейный характер ее целевой функции, который, конечно, не может соответствовать реальным условиям. По этой причине модель Гросса, учитывая ее простоту, использовано только для аппроксимации целевой функции и получения результатов в первом приближении.

Еще одной математической моделью, которая дает возможность рассчитать уровень убытков вследствие реализации угроз, зависит от объема затрат на защиту информации и КрБ являются модели, описанные в работах [20, 23, 25]. Целью исследований [20, 25] являлась оценка устойчивости комплекса технической защиты информации (ТЗИ) во времени с использованием известных распределений вероятностей [25].

При отсутствии финансовых инвестиций в защиту или его модернизацию вероятность надежности защищенности равна нулю независимо от времени. Данная модель позволяет установить зависимость вероятность защищенности от максимально эффективного финансирования.

Основные трудности при построении модели связаны со сбором статистических данных о результатах взлома (и необходимость факта самого излома защиты), поскольку такая система защиты после этого не может использоваться в дальнейшем. В связи с этим автором [18, 25] разработан метод для определения вероятностной надежности ТЗИ на основе реальных попытках взлома, который позволяет оценить вероятностную надежность одиночных систем защиты и при ее установке на нескольких объектах (например, установки антивирусной программы на нескольких компьютерах позволяет предусмотреть не только попытку, но и время, при котором возможен взлом на других компьютерах). Недостатком этого метода является необходимость знания эффективности ТЗИ, которая в данном случае получается в результате анализа последствий реального взлома системы.

В результате исследований, выполненных в работах [18, 20, 24, 25], авторы показали, что параметр, который определяет свойства ТЗИ, может быть не только постоянной величиной, но и функцией. Причем данная функция будет зависеть от попыток взлома и от времени, когда такие попытки имеют место, например, при тактике подбора паролей в ходе процедуры аутентификации пользователя в сети объекта информатизации. На основе исследований получены функции, позволяющие рассчитать частоту попыток взлома.

Модель Глушака - Новикова [26] направлена на оптимальное размещение механизмов защиты между компонентами (объектами) системы, которая обеспечит максимальный уровень защищенности.

Поиск оптимального набора механизмов защиты, который обеспечивает минимум риска потерь информации, проводится на примере системы районных отделений распределённого территориально объекта информатизации (автор рассматривал пример отделения банка). Объем информации в каждом отделении пропорционален потенциальному количеству клиентов, то есть численности жителей района. Вероятность реализации отдельных угроз, а также стоимость и эффективность каждого из механизмов защиты определяется методом экспертной оценки. При этом предполагается, что вероятность реализации угрозы для каждого объекта одинакова и зависит только от вида угрозы. Рассматривая различные комбинации элементов защиты для каждого из территориальных отделений, рассчитывается суммарный ущерб для всей системы (который и характеризует степень риска) и оптимальный набор элементов защиты для каждого отделения. При этом предусмотрена проверка условия введения ограничения на общую стоимость системы защиты.

При расчете полного риска остается открытым вопрос о величине перекрестных членов уравнений [26], которые выражают размер ущерба от реализации различных видов угроз (эти события считаются совместимыми).

Вопросам применения экономико-стоимостных моделей «атака-защита» для оценки рисков и исследования эффективности инвестиций в информационную безопасность посвящены работы О.Е. Архипова [27]. Для определения вероятностных параметров риска в этих моделях используются определенные характеристики мотивационно-стоимостных и экономико-финансовых отношений, характерных для ситуации «атака-защита» в информационной сфере. В частности, рассмотрена ситуация, возникающая при реализации атакующей стороной A (злоумышленник) угрозы T относительно некоторого информационного ресурса I, принадлежит стороне B.

Приведенные в работах [20, 25, 27] модели авторы предлагают применять непосредственно для вычисления рисков любой конкретной организации при условии, что существуетреальная возможность проанализировать и количественно оценить экономико-стоимостные характеристики реализации угрозы информации. Выходные данные для этих оценокможно получить, выполнив обследование (аудит) состояния информационной безопасности организации в соответствии с установками и рекомендациями стандартовменеджмента рисков при наличии определенной дополнительной информации, статические во времени оценки можно развить в динамические, изменяющие свои значения во временив соответствии с принятыми экономико-стоимостных сценариев развития атак.

Экономико-стоимостные модели «атака - защита» также дают возможность на основе конкретной информации о реальной организацию проверить, достаточнып объему средства, инвестированные в информационную безопасность этой организации.

Исследованию кибератак на информационные системы посвящены работы Хорошко В.А. [28]. Оценка возможностей злоумышленника при кибератаках проводится с использованием игровых методов анализа [28].

При формализации оптимального цикла кибератаки на информационную сферу предполагается оперирования понятие равновесия НэшаВ.

Заметим, что в данной модели не учтено влияние инвестиций на выбор оптимального решения, однако, исследователи демонстрируют как разработанные игровые методы анализапозволяют оценивать, как одиночные, так и групповые кибератаки.

Это позволяет получать гарантированные и достоверные оценки уровня защищенности информации от кибератак на информационную сферу, например, учебного заведения [1, 11].

Развитие экономических отношений и информационной сферы, в частности в области образования, приводит к усилению конкурентной борьбы, увеличению объемов и стоимости информации, а также потенциальных убытков от ее

утечки, росту количества информационных объектов (в ИОСУ это особенно заметно и динамично), частоты киберинцидентов. При этом условия противостояния постоянно меняются, отражая динамическое взаимодействие двух противоположных сторон – стороны защиты информации и стороны атакующих. Изменения стратегии и тактики стороны киберзащиты, вызывают новые атаки на информационные ресурсы, которые, с одной стороны, проявляют намерения соперника, с другой, указывают на слабые места защиты, на которые, как правило, направлены атаки или иные попытки деструктивного вмешательства. Другими причинами изменений в подходах к обеспечению ИБ и КрБ ИОСУ могут стать факторы, связанные с «устареванием» информации, введением новой информации и дополнительных ресурсов, перераспределением информационных ресурсов между объектами, появление новых связей между ними.

Антагонистическое противостояние двух сторон (стороны защиты и нападения) в информационной сфере характеризуется тем, что защита, как правило, находится в неопределенности относительно действий и финансовых возможностей противника (хакера). В тоже время, атакующие имеют некоторое представление о структуре системы защиты и могут направлять свои усилия на взлом наиболее слабых звеньев системы безопасности. Что даст атакующим наибольший эффект. Распределение ресурсов защиты на блокирование различного типа угроз может вестись как в активном режиме - опережая действия соперника, так и в адаптивном, с задержкой инвестирования, когда оказывается понятным направление возможных атак.

Заметим, что необходимость динамического управления ресурсами обусловлена следующими причинами:

– неопределенностью вариантов действий соперника, а именно направленностью его усилий по получению информации и масштабом этих усилий, которые в частности зависят и от финансовой компоненты ресурсов хакеров, затраченных на взлом;

– изменением со временем как внутренних, так и внешних условий противостояния - стоимости информации, ее распределения между объектами, направленности атак противника, появлением новых атакующих;

– изменением состояния информационной системы (ИОСУ рассматривается как частный случай), в частности, изменением ее самого слабого звена после обнаружения нацеленности атак и принятиясоответствующих мер со стороны защиты.

Анализ научных работ по математическому моделированию систем защиты информации показал, что основные усилия сосредоточены на определении объемаинвестиций в защиту.

Вопросам распределения этих инвестиций между объектами защиты посвященные единичные работы. Кроме того, существующие разработки [13, 17] редко учитывают влияние возможных действий злоумышленника и их последствий на изменение показателей и характеристик системы.

Таким образом, выполненный анализ работ в исследуемой тематике, показал, что задача эффективного использования ограниченных финансовых ресурсов на защиту информации субъектов хозяйственной деятельности и учебных заведений в частности, становится все более важной и в значительной [1, 4, 7, 11].

Развитие компьютерных систем и информационных технологий породило отдельную концепцию работ по оптимизации инвестирования в СКБ. Эта концепция исследований базируется на широком использовании экспертных систем (ЭС) [11] и СПР в задачах определения рациональных стратегий инвестирования в области КБ. Мы изучили достаточно много работ в этой области и пришли к выводу, что большая часть данных публикаций [11, 17], не содержит конкретных решений по выбору рациональных стратегий взаимного финансового инвестирования в СКБ ОУ.

Также, как следует из выводов работ [8, 9] и [11, 12], использование ЭС и СПР для автоматизации процедур выбора рациональных стратегий управления инвестированием в СКБ, не всегда сопровождается четкими рекомендациями.

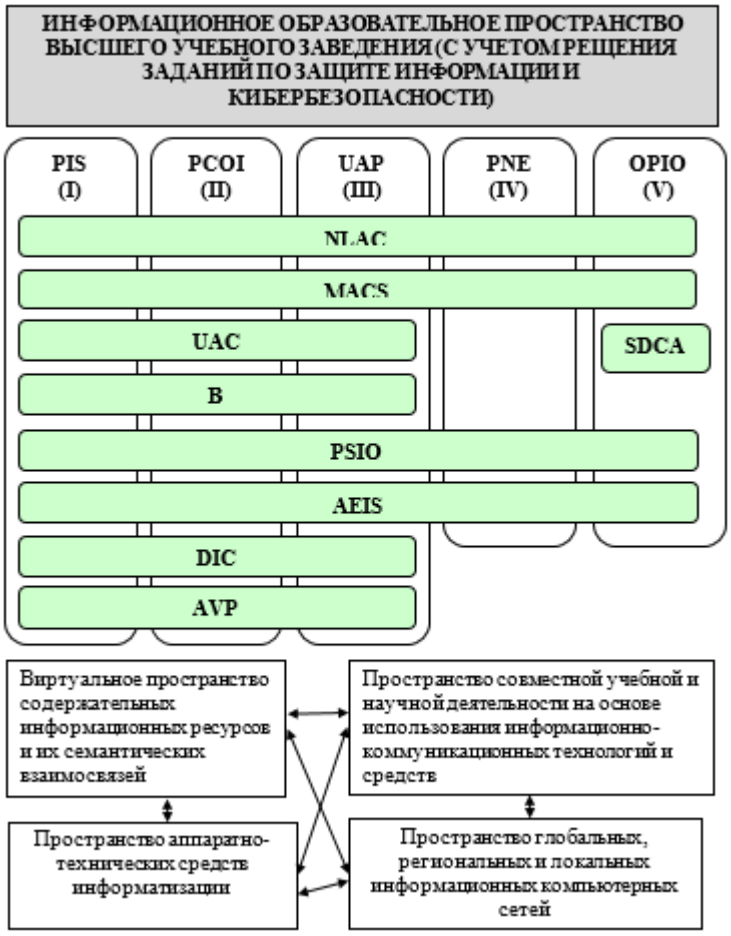
Данные обстоятельства и обусловили проблему, связанную с необходимостью разработки новых моделей для СПР в задачах определения рациональных стратегий взаимного финансового инвестирования в СКБ ОУ.

Опираясь на предшествующий опыт и подходы, изложенные авторами в более ранних публикациях по данной тематике [29], а также близкие по методологии исследований работы сторонних авторов [19, 25], можем утверждать, что достаточно эффективным подходом в решении подобного класса задач, является использование методов теории дифференциальных игр качества с несколькими терминальными поверхностями [17, 18].

Таким образом, анализ публикаций по данной тематике подтвердил релевантность проблемы дальнейшего развития моделей для СПР в задачах непрерывного взаимного инвестирования в СКБ ОУ. Последнее особенно важно для случаев, когда необходимо выработать четкие рекомендации для инвесторов. Но при этом нет необходимости применять сложные математические выкладки, т.к. большая часть вычислений выполняется компьютерными программами.

Основной материал статьи.

С учетом трактовки ИОСУ, приводимого разными авторами, возможно видоизменение ее структуры с учетом проблематики обеспечения киберзащищённости. Таким образом предлагается такая структура защищенной ИОСУ и, соответственно информационно-образовательного пространства университета, см. рис. 1.



Приняты следующие обозначения: AVP – antivirus protection; DIC – data integrity control; AEIS – audit of events of information security; PSIO – physical security of information object; B – backup; UAC – user access control; SDCA – subsystem of detection of cyber attacks; MACS – Monitoring and; analysis of cyber security; NLAC – Network-level access control.

Периметры КрБИОСУ:PIS (I) – The perimeter of the information system; PCOI (II) – Perimeter of control of object of informatization; UAP (III) – User Access Perimeter; PNE (IV) – The perimeter of the network equipment; OPIO (V) – The outer perimeter of information object.

Рис. 1. Структура защищённого информационного образовательного пространства вуза

Естественно, построение такой сложной организационной структуры как защищенная ИОСУ (далее ЗИОСУ) требует достаточно больших финансовых средств, которыми еще надо грамотно распорядится.

Процедура инвестирования в инновационные проекты, в частности в сфере развития цифровых технологий образования с акцентом на формирование информационно-образовательной среды (ИОС) ОУ, зачастую характеризуются высокой степенью неопределенности и рискованности в вопросах обеспечения кибербезопасности ОУ. Изменившийся за последние годы ландшафт киберугроз [21, 22], коренным образом повлиял на

отношение к проблематике КБ многих ОУ [11, 12]. Прежде всего, это было обусловлено, значительными потенциальными уязвимостями и киберугрозами для ИОС ОУ, появлением новых классов кибератак, широким распространением беспроводных технологий передачи данных и др. В условиях стремительного внедрения цифровых технологий в образовании далеко не все инвесторы, например, при создании частных и, в том числе, крупных международных университетов в РФ, Украине, Казахстане уделяли должное внимание проблематике КБ ИОС ОУ [11, 12, 15]. Заметим также, что не многие публикации в данной области содержат описание моделей, связанных с нахождение разно вариантных стратегий во взаимном финансовом инвестировании ОУ в СКБ [13, 14].

Для повышения результативности при оценивании различных инвестиционных проектов в СКБ ОУ, и последующего принятия решений, связанных с инвестированием, необходимо задействовать современные информационные технологии [15]. Например, технологии, которые базируются на применении систем поддержки решений (СПР) [18].

Наполнение информационно-алгоритмической составляющей СПР можно реализовать посредством введения блоков, которые содержат алгоритмы для математических моделей по инвестированию в СКБ ОУ.

Заметим, что несмотря на общность задач по КрБ для различных объектов информатизации (далее ОБИ, принято, что ОБИ – может быть ИОСУ, автоматизированная система управления сложным производством или банковская система), каждый из них имеет свою специфику киберугроз [1-5]. Однако, общей первоначальной задачей при построении эффективных систем защиты и КрБ любого ОБИ, остается задача обследования конкретного объекта защиты, формирование моделей потенциального нарушителя (компьютерного злоумышленника – КЗЛ) и киберугроз [1-5]. Реализация вышеуказанных шагов позволит в конечном итоге получить адекватные требования к системам защиты информации (СЗИ) ОБИ и ИОСУ, как частного случая.

В условиях усложнения сценариев кибератак на ИОСУ аналитикам служб информационной безопасности университетов и других учебных заведений необходимо достаточно оперативно реагировать на кибератаки, аномалии угрозы. Это делает актуальной задачу поиска новых способов повышения результативности принятия решений в заданиях реагирования на попытки деструктивного вмешательства со стороны КЗЛ или недобросовестного персонала университетов в работу ОБИ. И в такой ситуации значительную роль могут сыграть различные интеллектуализированные системы поддержки решений (ИСПР) и экспертные системы (ЭС) в заданиях обеспечения киберзащиты ОБИ [5-7].

Математической составляющей ИСПР и ЭС в задачах КрБ, являются различные модели и алгоритмы, дающие возможность специалистам интеллектуализировать поддержку решений. В рамках исследования рассмотрена возможность синтеза аналитических моделей для основных видов несанкционированного доступа к ресурсам ИОСУ [18, 30-32].

Выводы:

Проведен обзор и анализ предшествующих исследований в сфере обеспечения защиты информационно-образовательной среды университетов (ИОСУ);

показано, что приоритетность развития цифровых систем образования во многих промышленно развитых государствах мира требует соответствующей технико-методологической поддержки специалистов не только в области педагогической деятельности, но и информационных технологий с учетом проблематики кибербезопасности и защиты информации; обосновано, что сформированный во многих странах тренд на глобализацию доступа к информационным ресурсам делает релевантными задачи внедрения новейших цифровых и информационно-коммуникационных технологий во все сферы деятельности современного вуза; обоснована актуальность исследований в направлении разработки моделей для систем поддержки решений по нахождению стратегий управления инвестированием для различных соотношений параметров инвестиционного процесса в системы кибербезопасности образовательных учреждений; показана необходимость компьютерной поддержки решения задач по нахождению стратегий управления инвестированием в стратегии кибербезопасности образовательных учреждений; обоснована необходимость разработки концептуальной модели адаптивного управления киберзащитой объекта информатизации на примере ИОСУ.

ЛИТЕРАТУРА

[1]. Е. Бидайбеков, О подготовке специалистов по информатике и информатизации образования в Республике Казахстан, *Технология высшего образования в*

XXI веке: проблемы и перспективы развития: сб. материалов международной научно-практической конференции, Актобе: АГУ им. К. Жубанова, С. 62-65, 2002.

[2]. М. Нургужин, Б. Ахметов, А. Кулик, "Информационная образовательная среда университета", *Вестник МГПУ*, М.: МГПУ, №1, С. 228-233, 2006.

[3]. К. Нургалиева, Д. Сулеев, Ж. Тусубаева, *Технология организации дистанционной формы обучения, монография,* Алматы: Республиканский Центр информатизации образования, 2002, 50 с.

[4]. К. Абдиев, Статистические базы данных для информационных систем управления образованием, *Вестник АГУ им. Абая. Физико-математическая серия*, № 1(5), С. 7-10, 2002.

[5]. Б. Ахметов, В. Яворский, "Автоматизированная система рейтинговой оценки и анализа учебы студентов", *Новости науки Казахстана*, №3, С. 29-36, 2006.

[6]. Б. Ахметов, В. Яворский, "Автоматизированная аттестация и анализ деятельности профессорско-преподавательского состава университета", В*естник Павлодарского государственного университета им. С.Торайгырова*, №4, С. 47-50, 2005.

[7]. Б. Ахметов, К. Цхай, "Информационная образовательная среда вуза как основа системы дистанционного обучения", *Состояние и стратегия развития дистанционного образования в условиях глобализации: сб. материалов Международной конференции*, Караганда, С. 195-197, 2003.

[8]. Y. Rezgui, M. Adam, "Information security awareness in higher education: An exploratory study", *Computers & Security* 27.7, 2010, pp. 241-253.

[9]. N. Sultan, "Cloud computing for education: A new dawn? ", *International Journal of Information Management*, 30.2, pp. 109-116.

[10]. Б. Ахметов, В. Яворский, *Моделирование информационной образовательной среды вуза*, 2006, 251 с.

[11]. F. Schneider, "Cybersecurity education in universities", *IEEE Security & Privacy*, 11.4, pp. 3-4, 2013.

[12]. A. Conklin, "Cyber defense competitions and information security education: An active learning solution for a capstone course", *System Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on. Vol. 9. IEEE*, 2006.

[13]. M. Schuett, M. Rahman, *Information Security Synthesis in Online Universities,* arXiv preprint arXiv:1111.1771-2011.

[14]. N. Mariusz, M. Benton, *Cybersecurity cost of quality: managing the costs of cybersecurity risk management*. [Electronic recource]. Online: https://arxiv.org/ftp/arxiv/papers/1707/1707.02653.pdf-2017.

[15]. M. Jalali, M. Siegel, S. Madnick, *Decision making and biases in cybersecurity capability development: evidence from a simulation game experiment*. [Electronic resource]. Online: https://arxiv.org/ftp/ arxiv/ papers/ 1707/ 1707.01031.pdf-2017.

[16]. L. Gordon, M. Loeb, ,L. Zhou, "Investing in cybersecurity: insights from the Gordon-Loeb model", *J. Inf. Secur.* 7(02), 49, 2016.

[17]. B. Akhmetov, V. Lakhno, Y. Boiko, A. Mishchenko, "Designing a decision support system for the weakly formalized problems in the provision of cybersecurity", *Eastern-European Journal of Enterprise Technologies*, 1(2(85)), pp. 4-15, 2017.

[18]. V. Lakhno, Y. Boiko, A. Mishchenko, V. Kozlovskii, O. Pupchenko, "Development of the intelligent decision-making support system to manage cyber protection at the object of informatization", *Eastern-European Journal of Enterprise Technologies* 2/9 (86), pp. 53-61, 2017.

[19]. Р. Прус, "Вибірцільовоїфункції та їївплив на розподіл ресурсів захисту інформації", *Защита информации*, №16, С. 172-175, 2009.

[20]. Р. Прус, А. Сільченко, "Модель визначення об'єктів та засобів захисту підприємства від загроз", *Защита информации*, №16, С. 192-195, 2009.

[21]. Microsoft Security Intelligence Report VOLUME 23 Online: https:// info. microsoft. com/ww-landing-Security-Intelligence-Report-Vol-23-Landing-Page-eBook.html);

[22]. Cisco 2018 AnnualCybersecurityReport. Online: https://www.cisco.com/c/en/us/products/security /security-reports.html#download-report).

[23]. L. Gordon, M. Loeb, "Returnon Information Security Investments: Myths vs. Reality", *StrategicFinance*, pp. 26-31, 2002.

[24]. L. Gordon, M. Loeb, "The Economics of Information Security Investment", ACM Transactionson *Information and System Security*, vol. 5, no. 4, pp. 438-457, 2002.

[25]. А. Рабчун, "Аналіз статистики нападів в сфері інформаційної безпеки", *Вісник Інженерної академії України*, №2, С. 18-27, 2010.

[26]. В. Глушак, О. Новіков, "Синтез структури системи захисту інформації з використанням позиційної гри захисника та зловмисника", *Системні дослідження та інформаційні технології*, №2, С. 89-100, 2013.

[27]. А. Архипов, "Применение экономико-мотивационных соотношений для оценивания вероятностных параметров информационных рисков", *Захист інформації*, №2, С.69-76, 2011.

[28]. Р. Грищук, С. Піскун, В. Хорошко, Ю. Хохлачова, "Ігрові методи аналізу кібератак на інформаційну сферу", *Захист інформації*, №1, 2012.

[29]. Л. Кидираліна, Б. Ахметов, В. Лахно, "Моделювання процедури прийняття рішень щодо фінансування засобів кібербезпеки інформаційно-освітнього середовища університету", *Захист інформації*, №2, С. 120-127, 2018.

[30]. B. Akhmetov, V. Lakhno, B. Akhmetov, Y. Myakuhin, A. Adranova, L. Kydyralina, "Models and Algorithms of Vector Optimizationin Selecting Security Measures for Higher Education Institution's Information Learning Environment", *In Proceedings of the Computational Methodsin Systems and Software, Springer, Cham*, pp. 135-142, 2018.

[31]. B. Akhmetov, V. Lakhno, B. Akhmetov, Z. Alimseitova, "Development of Sectoral Intellectualized Expert Systems and Decision Making Support Systemsin Cybersecurity", *In Proceedingsofthe Computational Methodsin Systems and Software , Springer, Cham.* -pp. 162-171, 2018.

[32]. V. Lakhno, "Information Technologies for Maintaining of Management Activityof Universities", *Tretynyk InInternational Conferenceon Theory and Applications of Fuzzy Systems and Soft Computing, Springer, Cham,* pp. 663-672, 2018.

ПЕРЕДУМОВИ ДЛЯ ФОРМУВАННЯ БЕЗПЕЧНОГО ІНФОРМАЦІЙНО-ОСВІТНЬОГО СЕРЕДОВИЩА СУЧАСНОГО УНІВЕРСИТЕТУ

В роботі проведено огляд та аналіз попередніх досліджень у сфері забезпечення захисту інформаційно-освітнього середовища університетів (ІОСУ). Показано, що пріоритетність розвитку цифрових систем освіти в багатьох промислово розвинених державах світу вимагає відповідної техніко-методологічної підтримки фахівців не тільки в галузі педагогічної діяльності, а й інформаційних технологій з урахуванням проблематики кібербезпекита захисту інформації. Показано, що до інформації, якапотребує захисту та зберігається, а також циркулює в інформаційно-комунікаційних системах університетів, зокрема можна віднести: персональні дані учнів, викладачів, наукових співробітників, допоміжного персоналу; цифрована інформація, що представляє інтелектуальну власність навчального закладу; інформаційні масиви, які, забезпечують навчальний процес, (наприклад, мультимедійний контент, бази даних, навчальні програми); ін. Обґрунтовано, що дані інформаційні ресурси можуть виступити як об'єкт розкрадання або спотворення з боку зовнішніх (внутрішніх) комп'ютерних зловмисників або з хуліганських спонукань, з боку учнів або співробітників. Обґрунтовано, що сформований у багатьох країнах тренд на глобалізацію доступу до інформаційних ресурсів робить релевантними завдання впровадження новітніх цифрових і інформаційно-комунікаційних технологій в усі сфери діяльності сучасного університету. Обґрунтовано актуальність досліджень в напрямку розробки моделей для систем підтримки рішень по знаходженню стратегій управління інвестуванням для різних співвідношень параметрів інвестиційного процесу в системи кібербезпеки освітніх установ.

Ключові слова: кібербезпека, інформаційно-освітнє середовище університету, багатокрокова гра якості, оптимальні стратегії фінансування.

PREREQUISITES FOR THE FORMATION OF A SAFE INFORMATION-EDUCATIONAL ENVIRONMENT OF A MODERN UNIVERSITY

The paper reviewed and analyzed previous research in the field of protection of the information-educational environment of universities (ILE). It is shown that the priority development of digital education systems in many industrialized countries of the world requires appropriate technical and methodological support of specialists not only in the field of pedagogical activity, but also information technology, taking into account the problems of cyber security and information protection. It is shown that the protected data that is stored and circulate in the information and communication systems of universities, in particular, include: personal data of students, teachers, researchers, support staff; digitized information representing the intellectual property of the educational institution; information arrays that provide the learning process (for example, multimedia content, databases, training programs, etc.); It is substantiated that these information resources can act as an object of theft or distortion from external (internal) computer intruders or from hooliganism, from students or employees. It has been substantiated that the trend towards globalization of access to information resources, formed in many countries, makes relevant the task of introducing the latest digital and information and communication technologies in all areas of activity of a modern university. The relevance of research in the direction of developing models for decision support systems for finding investment management strategies for various ratios of the parameters of the investment process in the cybersecurity systems of educational institutions is substantiated.

Keywords: cybersecurity, information and educational environment of the university, multi-step quality game, optimal funding strategies.

Кыдыралина Лазат Муктаровна, докторант Казахского национального педагогического университета имени Абая, (Алматы, Казахстан).
E-mail: Lazat_75@mail.ru.

Кидираліна Лазат Муктаровна, докторант, Казахського національного педагогічного університету імені Абая, (Алмати, Казахстан).

Kydyralina Lazat, doctoral of Abai Kazakh National Pedagogical University, (Almaty, Kazakhstan).