ТЕХНИЧЕСКИЕ НАУКИ
И ТЕХНОЛОГИИ

АҚПАРАТТЫҚ ЖҮЙЕЛЕР
ИНФОРМАЦИОННЫЕ СИСТЕМЫ
INFORMATION SYSTEMS

DOI 10.51885/1561-4212_2023_2_21
МРНТИ 44.29.01

Ж.К. Алимсеитова[1], Б.С. Ахметов[2], Е.Т. Каламан[3]
[1]Сатпаев университет, г. Алматы, Казахстан
*E-mail: zhuldyz_al@mail.ru**
[2]Казахский национальный педагогический университет имени Абая, г. Алматы, Казахстан
E-mail: bakhytzhan.akhmetov.54@mail.ru
[3]Сатпаев университет, г. Алматы, Казахстан
E-mail: politeh.kalaman@gmail.com

ЦЕННОСТЬ ИНФОРМАЦИОННЫХ АКТИВОВ УЧЕБНЫХ ЗАВЕДЕНИЙ И ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИХ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ

ОҚУ ОРЫНДАРЫНЫҢ АҚПАРАТТЫҚ АКТИВТЕРІНІҢ ҚҰНДЫЛЫҒЫ ЖӘНЕ ОЛАРДЫҢ КИБЕРНЕТИКАЛЫҚ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУ МӘСЕЛЕЛЕРІ

THE VALUE OF INFORMATION ASSETS OF EDUCATIONAL INSTITUTIONS AND THE PROBLEMS OF ENSURING THEIR CYBERNETIC SECURITY

Аннотация. *В работе показано, что несмотря на то, что количество публикаций, посвященных кибернетической безопасности (КБ), из года в год стремительно растет, исследований, затрагивающих вопросы обеспечения КБ информационно-образовательной среды университетов (ИОСУ) и их компьютерных сетей, крайне мало. Показано, что необходимо продолжать исследования в направлении развития методов обеспечения КБ ИОСУ. Такие исследования помогут не только устранить уязвимости в контурах КБ ИОСУ, но и по-новому взглянуть на риски КБ для университетов. Также показано, что актуальны новые исследования в направлении изучения и категоризации информационных активов университетов и колледжей, с учетом специфики подготовки кадров в системе высшего образования Республики Казахстан. Это позволит получить новую информацию, необходимую для изучения ценности информационных активов в высшем образовании, что будет способствовать построению более безопасных компьютерных систем и сетей, используемых в учебном процессе и межакадемическом обмене научной информацией.*

Ключевые слова: *кибернетическая безопасность, информационно-образовательная среда университетов, информационные активы, риски, информационно-коммуникационные сети.*

Аңдатпа. *Жұмыста жыл сайын кибернетикалық қауіпсіздікке (КҚ) арналған басылымдардың саны тез өсіп келе жатқанына қарамастан, университеттердің ақпараттық-білім беру ортасын (УАББО) және олардың компьютерлік желілерінің КҚ қамтамасыз ету мәселелерін қозғайтын зерттеулер өте аз екендігі көрсетілген. УАББО КҚ қамтамасыз ету әдістерін дамыту бағытында зерттеулерді жалғастыру қажет екендігі көрсетілген. Мұндай зерттеулер УАББО КҚ контурларындағы осалдықтарды жоюға ғана емес, сонымен қатар университеттер үшін КҚ тәуекелдеріне жаңа тәсілдермен қарастыруға көмектеседі. Сондай-ақ, Қазақстан Республикасының Жоғары білім беру жүйесінде кадрлар даярлау ерекшелігін ескере отырып, университеттер мен колледждердің ақпараттық активтерін зерделеу және санаттарға бөлу бағытында жаңа зерттеулердің өзекті екендігі көрсетілген. Бұл жоғары білім берудегі ақпараттық активтердің құндылығын зерттеу үшін қажетті жаңа ақпаратты алуға мүмкіндік береді. Бұл өз кезегінде оқу процесінде және академиялық ақпарат алмасуда қолданылатын қауіпсіз компьютерлік жүйелер мен желілерді құруға ықпал етеді.*

Түйін сөздер: *кибернетикалық қауіпсіздік, университеттердің ақпараттық-білім беру ортасы,*

ақпараттық активтер, тәуекелдер, ақпараттық-коммуникациялық желілер.

Abstract. *The paper shows that despite the fact that the number of publications devoted to cybernetic security (CC) is growing rapidly from year to year, research affecting the issues of ensuring the CC of the information and educational environment of universities (IEEU) and their computer networks are extremely small. It is shown that it is necessary to continue research in the direction of the development of methods for providing CC IEEU. Such studies will help not only to eliminate vulnerabilities in the contours of the IEEU Design Bureau, but also to take a fresh look at the risks of design bureaus for universities. It is also shown that new research is relevant in the direction of studying and categorizing information assets of universities and colleges, taking into account the specifics of personnel training in the higher education system of the Republic of Kazakhstan. This will provide new information necessary to study the value of information assets in higher education. And this, in turn, will contribute to the construction of more secure computer systems and networks used in the educational process and inter-academic exchange of scientific information.*

Keywords: c*ybernetic security, information and educational environment of universities, information assets, risks, information and communication networks.*

Введение. Стремительное технологическое развитие и широкое применение информационных технологий (ИТ) в системе образования, в том числе высшего, свидетелями и участниками которых является весь мир, увеличивают долю киберугроз и киберпреступлений. Из-за пандемии, связанной с Covid-19, возникла глобальная зависимость от Интернета (это, например, касается таких направлений, как электронное правительство, электронная коммерция, дистанционное обучение и многое другое). А это, в свою очередь, дало компьютерным злоумышленникам широкие возможности для нарушения кибернетической безопасности (КБ) учебных заведений.

Многие университеты Казахстана в настоящее время находятся в процессе технологического развития своей информационно-образовательной среды [1] (ИОСУ). Доступ к информационным технологиям важен для развития современных ИОСУ. Но, с другой стороны, это увеличивает уязвимость информационно-коммуникационных сетей (ИКС) университетов, количество угроз при этом также растет. Так, например, в ряде исследований [2, 3, 4] показано, что кампусы многих колледжей и университетов часто подвергаются компьютерным атакам. Это результат того, что именно кампусы стали одними из наиболее технологически развитых мест работы студентов. Информационно-коммуникационные сети кампусов обеспечивают расширенную поддержку Wi-Fi, онлайн-обучение на платформах Moodle, Platonus, Canvas, Daryn.online и др., подключение к цифровым библиотекам, классам виртуализации, веб-конференциям и т.п. Все это делает университетские сети весьма уязвимыми к внешним и внутренним атакам злоумышленников [1, 2, 4].

Сети Wi-Fi в учебных заведениях (колледжи, университеты и пр.) часто используют устаревшие протоколы передачи данных g/n и уже теряющий актуальность протокол IEEE 802.11 ac, поэтому скорость доступа к информации оставляет желать лучшего. В этом случае пользователи начинают пользоваться мобильным интернетом и включают точки раздачи Wi-Fi. Это способствует тому, что забиваются доступные каналы и еще больше уменьшается скорость передачи данных по беспроводной сети, а также радиус действия точек доступа в учебном заведении.

Что же касается сетевых хранилищ, используемых для дистанционного обучения, то они часто строятся на базе не предназначенных для этих целей серверов. Такие неспециализированные серверы не только не могут предоставить необходимую производительность при чтении/записи информации, но и не имеют резервирования питания дисковых контроллеров, что создает опасность потери важной информации, например, во время сессии.

В [1, 2, 4] авторами было показано, что организованная преступность, промышленный шпионаж и человеческие ошибки являются наиболее заметными факторами, влияющими на угрозы в сфере КБ университетов и колледжей. В свою очередь, эти угрозы могут использовать уязвимости в административных, технических и физических контурах ИБ

учебных заведений.

Внедрение системы управления КБ в университетах является важным шагом в обеспечении их общей информационной безопасности ИОСУ в целом. При всем вышеизложенном, исследования в области обеспечения ИБ компьютерных сетей университетов очень ограничены и не содержат конкретных деталей реализации, анализа эффективности применения систем КБ в вузах. А это делает наше исследование актуальным.

Цель работы. Целью работы является исследование связей между такими понятиями, как ценность информационных активов учебных заведений, прежде всего на примере университетов и колледжей, и проблематика обеспечения кибернетической безопасности их информационно-коммуникационных сетей. Это позволит получить новую информацию, необходимую для изучения ценности информационных активов в высшем образовании, и будет способствовать построению более безопасных компьютерных систем и сетей, используемых в учебном процессе и межакадемическом обмене научной информацией.

Материалы и методы исследования. Ландшафт киберугроз для университетов и колледжей динамично изменяется. Например, помимо «классических» угроз для информационных активов, в последние годы добавились угрозы, связанные с широким внедрением в учебный процесс интернета вещей, мобильных устройств и т.п. Кроме того, в университетах имеются и специфические угрозы. Это связано с достаточно свободным потоком рабочей силы, ведь многие преподаватели в рамках академической мобильности могут работать в разных университетах и колледжах. Каждый новый год в учебных заведениях происходит ротация студентов, гостей и других посетителей, что также может повлиять на состояние ИБ учебного заведения. Несмотря на то, что университеты и колледжи сталкиваются со значительными рисками в вопросах ИБ, инициативы менеджмента учебных заведений в этом направлении носят разную направленность [1]. Следовательно, создавая защищенную компьютерную сеть для университетов, необходимо решить комплекс как технических, так и организационных вопросов. Это позволит сбалансировать меры по информационной безопасности с академической открытостью и свободными потоками информации, которые присущи сфере образования во всем мире.

Как показал анализ ряда публикаций [3-8], университеты и колледжи часто располагают достаточно большими объемами ценных информационных активов, например результатов инновационных научно-технических разработок, особенно связанных с применением высоких технологий. Это делает компьютерные системы университетов привлекательной мишенью для киберпреступников.

Первичные информационные активы любой организации или компании, в том числе университетов и колледжей, – это информация либо бизнес-процессы, которые организация считает ценными. В этот перечень можно добавить здания, оборудование, персонал, репутацию учебного заведения, деловые документы (например, контракты или договора на обучение, бухгалтерская документация и т.п.) и другие материальные и нематериальные активы. С другой стороны, информационные активы – это «активы, которые собирают, хранят, обрабатывают или передают информацию, представляющую ценность для организации» [4-6].

Заметим, что важными принципами системы высшего образования (СВО), а следовательно, и таких его компонентов, как университеты и колледжи, являются академическая свобода и открытость. Академическая свобода определяется [2] как «свобода преподавателей и студентов преподавать, учиться и заниматься знаниями и исследованиями без необоснованного вмешательства или ограничений со стороны государственных законов, институциональных правил или общественного давления. В то время как другой прин-

цип, открытость, обычно описывается как всеобъемлющая концепция или философия, которая характеризуется акцентом на прозрачность и сотрудничество [3]. То есть, под открытостью понимается «доступность знаний, технологий и других ресурсов; прозрачность действий; проницаемость организационных структур; инклюзивность участия в образовательном процессе» [3].

Высшее образование в любом государстве выполняет важную социальную функцию, связанную с исследованиями, разработками и образованием. Академические исследования в основном ориентированы на совместную и командную работу, как междисциплинарную, так и многостороннюю. Автономия, индивидуальность и свобода выбора характеризуют среду СВО с небольшими ограничениями в отношении сотрудничества и распространения знаний и информации, касающейся научных исследований. Эти свойства отличаются от промышленности, где коммерческие секреты распространяются открыто и часто жизненно важны для успешного бизнеса. Цели подготовки специалистов в системе высшего образования, как правило, долгосрочны. Существенным аспектом высшего образования является и то обстоятельство, что исследовательская карьера индивидуальна.

В отличие от акцентов на кибербезопасность и секретность, которые присущи, например, финансово-банковской сфере и промышленности, академическая среда процветает благодаря открытости ученых в разных странах мира. Открытость, в свою очередь, основана на многовековых традициях доверия в академической среде, обмена информацией и дискуссиях ученых [4]. Таким образом, типичные характеристики информационно-образовательной среды университетов должны быть открытыми и всеобъемлющими. Это означает относительно небольшое количество физических периметров в контурах безопасности университетских помещений и относительно нестрогий контроль доступа, например, в компьютерные сети учебных заведений. Во многих университетах и колледжах учащиеся могут свободно подключаться к беспроводным сетям. Университеты и колледжи сталкиваются с ежегодным набором новых студентов, временных сотрудников и приглашенных преподавателей. В условиях автономности функционирования во многих университетах факультеты строят свои собственные компьютерные сети, предназначенные для поддержки исследований, разработок и преподавательской деятельности [5]. Подобного рода факультетские сети часто администрируют локально с низкой степенью централизованного контроля за состоянием их безопасности [5-7].

Как показал анализ ряда научных работ [5-13], количество исследований, посвященных информационным активам в университетах и колледжах, является весьма ограниченным. Причиной этого может быть сложность количественной оценки информационных активов в учреждениях системы высшего образования.

В работах [7, 8, 9-13] подчеркивается, что колледжи и университеты собирают самые разнообразные данные. Это могут быть данные студентов, родителей, абитуриентов, спонсоров, попечителей, членов правления, выпускников, преподавателей, персонала и др. Тип данных, которые собирают и хранят учебные заведения, разнообразен. Это могут быть как открытые данные, так и конфиденциальные, например, касающиеся финансовых, медицинских, личных, налоговых вопросов. Колледжи и университеты являются не только учреждениями высшего образования, но также финансовыми (каждый университет и колледж имеет собственную бухгалтерию и финансовый отдел), медицинскими учреждениями (многие университеты имеют в своих структурах поликлиники, профилактории, медицинские пункты и т.п.) и др. Таким образом, учебные заведения сегодня имеют широкий портфель информационных активов, учитывая разнообразие бизнес-процессов в сфере высшего образования. Стоимость актива является относительной и меняется в зависимости от продолжительности жизненного цикла угроз и их ландшафта

для ИОСУ. Также определённое влияние на стоимость информационных активов накладывают требования национальных законодательств разных государств и иные факторы.

Данные исследований, проводимых университетами, – это достаточно широкий термин. Например, его можно трактовать как «любую информацию, которая была собрана, наблюдалась, генерировалась или создавалась для подтверждения первоначальных результатов исследований» [4, 5, 6]. Данные исследований могут представляться, обрабатываться и храниться во многих форматах, и в первую очередь цифровых. Хотя ценность исследовательских данных различна, есть примеры, когда данные, полученные в ходе исследований, незаменимы. Некоторые исследовательские данные могут быть строго конфиденциальными (на такие данные может быть наложен гриф «секретно» или «совершенно секретно» и т.п.). В то же время другие данные требуют только выполнения обычных процедур, связанных с контролем целостности и/или доступности. Примерами данных исследований являются научные данные, академические знания, необработанные данные, результаты анализа и научных публикации и др. Кроме того, эта категория может включать такие активы, как данные управления исследованиями, проводимыми в универ-ситетах, контракты исполнителей и руководителей тем (в том числе закрытых), интеллек-туальная собственность, патенты, информация о финансировании и т.п. С учетом всего вышесказанного представляется необходимым более щепетильно подходить к вопросу проектирования или модернизации ИКС учебных заведений, делая акценты на ценность информационных активов и памятуя о рисках для информационной безопасности учебных заведений. Это особенно актуально при очевидном тренде на рост числа угроз и увеличивающуюся сложность проводимых кибератак, направленных на ИКС универси-тетов и колледжей.

Говоря о КБ в университетах и колледжах, невозможно обойти такой крайне важный аспект проблемы, как осведомленность учащихся о КБ в процессе обучения. Осведомленность студентов вузов о КБ исследовалась и до сих пор исследуется [14-16]. Так, в ряде публикаций [14, 16] было установлено, что основная проблема осведомленности о КБ в вузах заключается не в недостатке знаний о КБ (или ИБ), а в том, как учащиеся применяют эти знания в реальных ситуациях. Были даны рекомендации, чтобы помочь вузам в разработке учебных программ, включающих в себя обучение по повышению осведомленности о КБ применительно к реальным ситуациям. Было показано, что студенты вузов, несмотря на их уверенность в том, что за ними ведется наблюдение при использовании Интернета и что их данные не защищены даже в ИОСУ, не полностью осведомлены о том, как защитить свои данные [14].

Модель защищённой сети учебного заведения (рис. 1) показывает, что чем больше слоев защиты имеют данные (или информационные активы), тем сложнее злоумышленнику получить к ним доступ. Поэтому подавляющее число экспертов [1-8] рекомендуют строить сеть учебного заведения с несколькими уровнями аппаратной и программной защиты.

Кроме маршрутизаторов в сети обязательно должны быть файерволы, система распознавания вторжений и глубокого анализа трафика, а также локальная защита каждого устройства от атак на 2 и 3 уровнях модели OSI [1] (рис. 2).

Очень важной частью защищенной сети учебного заведения является резервирование устройств. Это предотвращает не только потерю доступа к ресурсам при выходе из строя определенного сетевого устройства, но и при атаке класса отказ обслуживания. Также важно подключение ключевых устройств сети (маршрутизаторов, файерволов и других систем защиты, коммутаторов ядра и серверов) к источникам бесперебойного питания и дизельных/бензиновых генераторов, способных запитать сеть даже при отключении цен-

тралізованного электроснабжения.

Одними из наиболее распространенных атак, направленных на ИКС университетов и колледжей, являются DDoS-атаки.

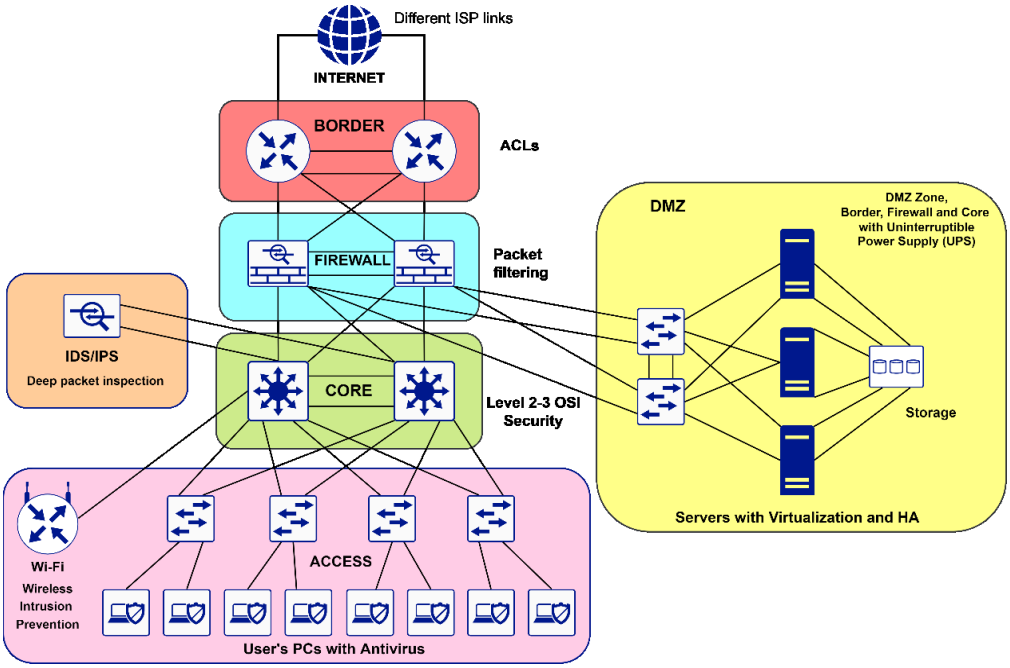

Рисунок 1. Модель защищенной локальной сети учебного заведения

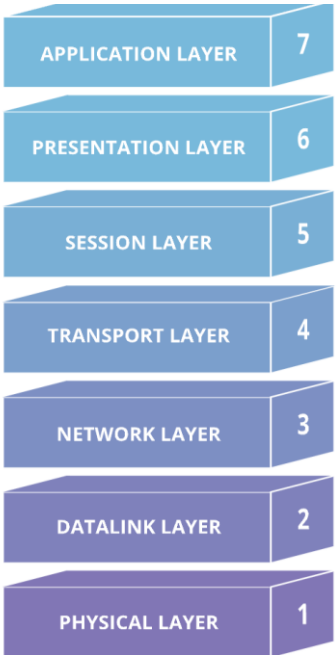

Рисунок 2. Модель OSI

Хотя почти все DDoS-атаки связаны с перегрузкой целевого устройства или университетской ИКС трафиком, подобные атаки можно разделить на три категории: атаки на

уровне приложений; атаки на уровне протокола; объемные атаки. Злоумышленник может использовать один или несколько различных векторов атаки или циклически использовать векторы атаки в ответ на применяемые контрмеры.

От атак 7-го уровня трудно защититься. Это связано с тем, что достаточно сложно отличить злонамеренный трафик от легитимного.

Сегодня к предоставлению ИТ-услуг в образовании и науке предъявляется серьезное требование – создание принципиально новой ИОСУ, обеспечивающей интерактивность, гибкость, мобильность и простой доступ к информационным и вычислительным ресурсам. С развитием современных ИТ (виртуализации, облачных технологий хранения данных, сетевого программного обеспечения, систем мониторинга состояния и кибербезопасности компьютерной сети) назрела необходимость перехода к динамической ИТ-инфраструктуре университета. Такой переход даст возможность поддерживать высокий уровень качества и доступности сервисов, гарантировать их динамичность и оперативность реагирования на изменения сервисов и ресурсов, обеспечивать непрерывность бизнес-процессов вуза при условии политики информационной безопасности, принятой в вузе.

В такой постановке к сетевой инфраструктуре университета применяются высокие требования по обеспечению надежных коммуникаций между пользователями и учебными корпусами, территориально-разделенных между собой, при многообразии и сложности используемого оборудования, различных режимов работы персонала.

Виртуальные локальные сети, созданные, например, в рамках одного факультета, уменьшают частоту коллизий и уменьшают количество бесполезных сетевых ресурсов, действуя как сегменты безопасной университетской ИКС. Пакеты данных, отправленные с рабочих станций в сегменте, передаются по мосту или коммутатору. Мост или коммутатор не перенаправляют коллизии, а рассылают широковещательные сообщения всем сетевым устройствам ИКС. По этой причине сегменты называются «доменами коллизий», поскольку они содержат коллизии внутри этого участка.

Первоначальные схемы дополнительных частей университетской ИКС могут изменяться в случае изменения нагрузки. Например, на рис. 3 изображена схема сети университетского корпуса с большой нагрузкой по трафику.

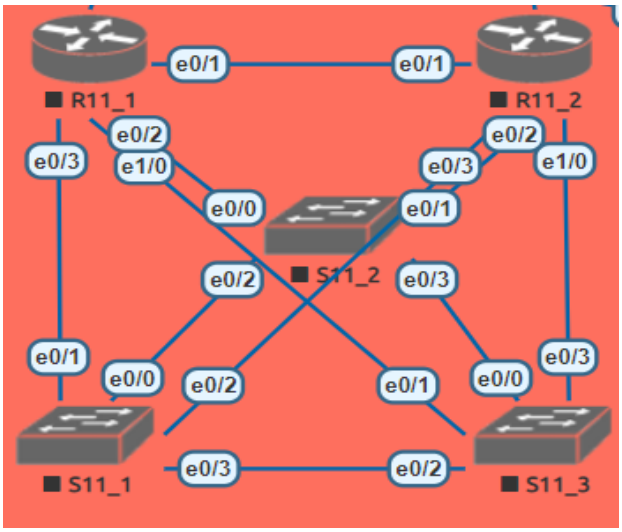

Рисунок 3. Схема сети университетского корпуса с большой нагрузкой

Заметим, что большая часть проанализированных научных публикаций [1, 3, 5, 9] поднимает вопросы защиты систем дистанционного обучения как наиболее уязвимого

сегмента ИОСУ. Вопросы ценности информационных активов при этом почти не затрагиваются, а акцент делается на социальную значимость дистанционного образования.

Открытая и разнообразная среда является стандартным требованием в высшем образовании. Вычислительная среда университета создается учеными для ученых, не осведомленных о проблемах кибербезопасности. Поэтому в большинстве случаев ИОСУ не хватает ресурсов для поддержания баланса между открытостью и безопасностью от вредоносного программного обеспечения, краж конфиденциальных данных и др.

Для проверки работоспособности защищенной сети учебного заведения (рис. 1) была выбрана платформа VmWare Workstation, установленная на компьютере под управлением ОС Windows 10. Сам компьютер построен на базе серверного процессора Intel Xeon E5 1650 и имеет установленную память ОЗУ объемом 32 Гб. Этого достаточно для операций по созданию ВМ и моделированию работы систем информационной безопасности. В общей сложности были созданы 3 виртуальные машины. Две – под управлением ОС Proxmox VE, выступающей гипервизором для развертывания на нем других виртуальных машин. На третьей ВМ установлена Ubuntu Server и приложение для моделирования сетей EVE-NG. Для создания ВМ было выбрано кастомизированное создание в настройках. Приложение Pi-Hole позволяет в режиме реального времени просматривать, какие запросы блокируются, а какие разрешаются в сети университета, выводить статистику в форме диаграмм и просматривать их детали (рис. 4).

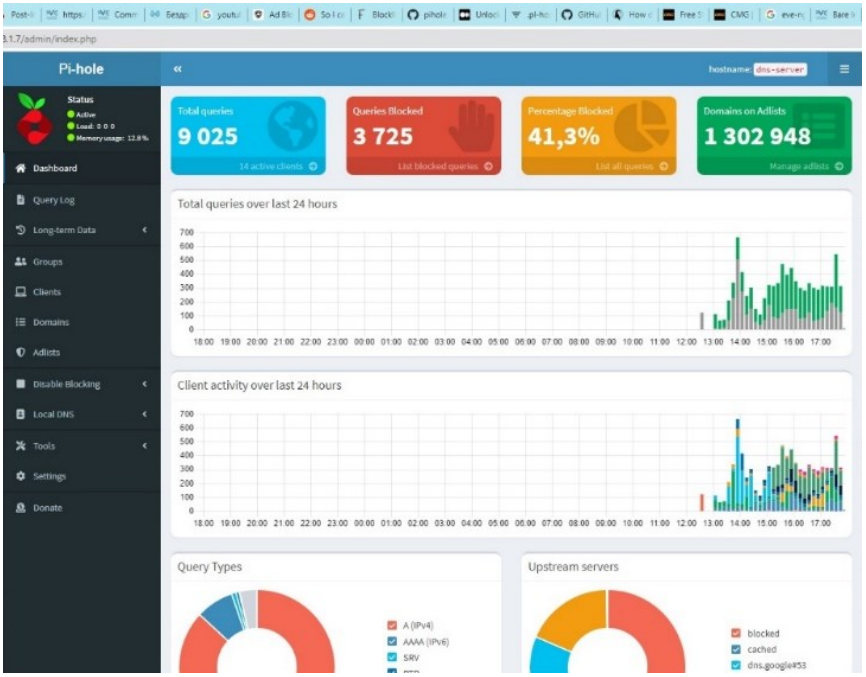

Рисунок 4. Общая статистика работы Pi-Hole

Из полученных результатов, показанных на рис. 4, видно, что система после модернизации, в соответствии со схемой, представленной на рис. 1, за 5 часов работы заблокировала более 3700 вредных запросов, что составляет более 41 % всего трафика, входящего в сеть учебного заведения.

Помимо общей информации о заблокированных угрозах, Pi-Hole предоставлял возможность просмотра информации о том, к каким запрещенным доменам идет

больше всего обращений, от которых клиентам идет больше всего запросов, как в целом, так и вредных в частности.

Заметим, что на данном этапе исследования акцент был сделан прежде всего на социальную значимость дистанционного образования и способы его защиты.

Заключение. Таким образом, даже предварительный анализ ситуации, связанной с проблематикой обеспечения ИБ компьютерных сетей учебных заведений, показал следующее:

1. Несмотря на то, что количество исследовательских работ по КБ стремительно растет, исследований, посвященных вопросу обеспечения КБ информационно-образовательной среды университетов и их компьютерных сетей, крайне мало.

2. Установлено, что организованная преступность, промышленный шпионаж и челове-ческие ошибки были наиболее заметными факторами, влияющими на угрозы в сфере КБ системы высшего образования. Эти угрозы могут использовать уязвимости в администра-тивных, технических и физических контурах ИБ учебных заведений.

3. Необходимо продолжать исследования в направлении развития методов обеспечения КБ ИОСУ, поскольку такие исследования помогут не только устранить уязвимости в контурах ИБ ИОСУ, но и по-новому взглянуть на риски КБ для университетов.

4. Показано, что актуальны новые исследования в направлении изучения и категоризации информационных активов университетов и колледжей, с учетом специфики подготовки кадров в системе высшего образования Республики Казахстан. Это позволит получить новую информацию, необходимую для изучения ценности информационных активов в высшем образовании, что, в свою очередь, будет способствовать построению более безопасных компьютерных систем и сетей, используемых в учебном процессе и межакадемическом обмене научной информацией.

Список литературы

1. Ахметов Б., Лахно В. Защита информации и кибербезопасность цифровой образовательной среды университета // Вестник КазАТК. – 2022. – № 120(1). – С. 134-141. – https://vestnik.alt.edu.kz/index.php/journal/article/view/346.
2. Ворожцова, Т.Н. Онтология как основа для разработки интеллектуальной системы обеспечения кибербезопасности // Онтология проектирования. 2014. – № 4. – С. 69-77. https://www.ontology-of-designing.ru/article/2014_4%2814%29/7_Vorozhtsova.pdf).
3. Yilmaz, R., Yalman, Y. A Comparative Analysis of University Information Systems within the Scope of the Information Security Risks // TEM J. – 2016. – № 5. – P. 180-191. – https://temjournal.com/content/52/TemJournalMay2016_180_191.pdf.
4. Adams, A., Blanford, A. Security and Online Learning: To Protect and Prohibit. In Usability Evaluation Of Online Learning Programs // IGI Global: Hershey, PA, USA. – 2003. – P. 331-359. – https://www.igi-global.com/gateway/chapter/30618.
5. Schneider, F. B. Cybersecurity education in universities // IEEE Security & Privacy. 2013. №11(4). P. 3-4. – https://ieeexplore.ieee.org/document/6573305/
6. Pawlowski, S. D., & Jung, Y. Social representations of cybersecurity by university students and implications for instructional design // Journal of Information Systems Education. – 2015. –№ 26(4). – P. 281-294.
7. Whitman, M. Management of Information Security. Cengage Learning, Inc.: Boston, MA, USA. – 2018. – ISBN 9780357691205.
8. Altbach, P. G. Academic freedom: International realities and challenges // Higher education. – 2001. – №41(1). – P. 205-219. – https://link.springer.com/article/10.1023/A:1026791518365
9. Peter, S., Deimann, M. On the role of openness in education: A historical reconstruction // Open Prax. – 2013. – №5. – P. 7-14. – https://openpraxis.org/articles/abstract/10.5944/openpraxis.5.1.23/
10. Chen, Y., He, W. Security risks and protection in online learning: A survey // Int. Rev. Res. Open Distrib. Learn. – 2013. – №14. – P. 108–127. –https://www.irrodl.org/index.php/irrodl/article/view/1632
11. Beaudin, K. The Legal Implications of Storing Student Data: Preparing for and Responding to Data Breaches // New Dir. Institutional Res. – 2017, 2016. – P. 37-48. – https://onlinelibrary.wiley.com/doi/10.1002/ir.20202.

12. Beaudin, K. College and university data breaches: Regulating higher education cybersecurity under state and federal law // J. Coll. Univ. Law. – 2015. – № 41. – P. 657-693.
13. Hussain, H.S., Din, R., Khidzir, N.Z., Daud, K.A.M., Ahmad, S. Risk and Threat via Online Social Network among Academia at Higher Education // J. Physics: Conf. Ser. – 2018, 1018, 012008.
14. Ulven, J. B., & Wangen, G. A systematic review of cybersecurity risks in higher education // Future Internet. – 2021. – №13(2). – P. 39. – https://www.mdpi.com/1999-5903/13/2/39.
15. Bongiovanni, I. The least secure places in the universe? A systematic literature review on information security management in higher education // Comput. Secur. – 2019. – No.86. – P. 350–357. – https://www.sciencedirect.com/science/article/pii/S0167404819301324?via%3Dihub.
16. Ncube, C.; Garrison, C. Lessons learned from university data breaches // Palmetto Bus. Econ. Rev. – 2010. – No. 13. – P. 27-37.

References

1. Ahmetov, B., & Lahno, V. Zashchita informacii i kiberbezopasnost' cifrovoj obrazovatel'noj sredy universiteta // Vestnik KazATK. – 2022. – № 120(1). – P. 134-141. – https://vestnik.alt.edu.kz/index.php/journal/article/view/346.
2. Vorozhcova, T.N. Ontologiya kak osnova dlya razrabotki intellektual'noj sistemy obespecheniya kiberbezopasnosti // Ontologiya proektirovaniya. – 2014. – № 4. – P. 69-77. – https://www.ontology-of-designing.ru/article/2014_4%2814%29/7_Vorozhtsova.pdf).
3. Yilmaz, R., Yalman, Y. A Comparative Analysis of University Information Systems within the Scope of the Information Security Risks // TEM J. – 2016. – № 5. – P. 180-191. https://temjournal.com/content/52/TemJournalMay2016_180_191.pdf.
4. Adams, A., Blanford, A. Security and Online Learning: To Protect and Prohibit. In Usability Evaluation Of Online Learning Programs // IGI Global: Hershey, PA, USA. – 2003. – P. 331-359. –https://www.igi-global.com/gateway/chapter/30618.
5. Schneider, F. B. Cybersecurity education in universities // IEEE Security & Privacy. – 2013. – № 11(4). – P. 3-4. – https://ieeexplore.ieee.org/document/6573305/
6. Pawlowski, S.D., & Jung, Y. Social representations of cybersecurity by university students and implications for instructional design // Journal of Information Systems Education. – 2015. – № 26(4). – P. 281-294.
7. Whitman, M. Management of Information Security. Cengage Learning, Inc.: Boston, MA, USA. – 2018. – ISBN 9780357691205.
8. Altbach, P. G. Academic freedom: International realities and challenges // Higher education. 2001. № 41(1). – P. 205-219. – https://link.springer.com/article/10.1023/A:1026791518365.
9. Peter, S., Deimann, M. On the role of openness in education: A historical reconstruction // Open Prax. – 2013. – №5. – P. 7-14. – https://openpraxis.org/articles/abstract/10.5944/openpraxis.5.1.23/
10. Chen, Y., He, W. Security risks and protection in online learning: A survey // Int. Rev. Res. Open Distrib. Learn. – 2013. – № 14. – P. 108-127. – https://www.irrodl.org/index.php/irrodl/article/view/1632
11. Beaudin, K. The Legal Implications of Storing Student Data: Preparing for and Responding to Data Breaches // New Dir. Institutional Res. – 2017, 2016. – P. 37-48. – https://onlinelibrary.wiley.com/doi/10.1002/ir.20202.
12. Beaudin, K. College and university data breaches: Regulating higher education cybersecurity under state and federal law // J. Coll. Univ. Law. – 2015. – № 41. – P. 657–693.
13. Hussain, H.S., Din, R., Khidzir, N.Z., Daud, K.A.M., Ahmad, S. Risk and Threat via Online Social Network among Academia at Higher Education // J. Physics: Conf. Ser. – 2018, 1018, 012008.
14. Ulven, J. B., & Wangen, G. A systematic review of cybersecurity risks in higher education // Future Internet. – 2021. – № 13(2). – P. 39. – https://www.mdpi.com/1999-5903/13/2/39.
15. Bongiovanni, I. The least secure places in the universe? A systematic literature review on information security management in higher education // Comput. Secur. – 2019. – No.86. – P. 350–357. – https://www.sciencedirect.com/science/article/pii/S0167404819301324?via%3Dihub.
16. Ncube, C.; Garrison, C. Lessons learned from university data breaches. // Palmetto Bus. Econ. Rev. – 2010. – No. 13. – P. 27-37.