УДК 004.056

Дусекеев Р.М.*, Мутанов Г.М., Мамыкова Ж.Д**.

Казахский национальный университет имени аль-Фараби, Республика Казахстан, г. Алматы
E-mail: *Ruslan.Dussekeev@kaznu.kz, **Zhanl.Mamykova@kaznu.kz

Роль информационной безопасности в развитии ИТ-инфраструктуры и повышении конкурентоспособности университета

В настоящее время сфера образования развивается необычайно динамично, приобретая новые черты, трансформируются ее функциональные, структурные, организационные, идеологические, ценностные характеристики. Кардинальные преобразования происходят в высшей школе. Все это порождает проблему поиска новых источников повышения конкурентоспособности вуза.

Статья посвящена роли информационной безопасности (ИБ) в повышении конкурентоспособности вузов. Уровень ИБ, наряду с основными показателями эффективности работы университетов, такими как: качество образовательного процесса, подготовка будущих специалистов-выпускников, количество и качество научных исследований, высококвалифицированный профессорско-преподавательский состав, является важным показателем, так как качество обеспечения информационной безопасности в вузе непосредственно влияет на репутацию и соответственно на его конкурентоспособность. На сегодняшний день в учреждениях высшего образования отсутствует формализованные процедуры, действия или меры по защите ИТ-инфраструктуры, нет управляющей модели обеспечения информационной безопасности.

В данной работе проведен анализ основных угроз безопасности информационных систем (ИС) вузов, на основании его результатов предлагается управляющая модель, которая может быть использована в качестве основы при создании собственной системы информационной безопасности университетов. Использование такой модели позволит эффективно предупреждать и заранее выявлять угрозы информационной безопасности ИТ-инфраструктуры и обеспечит надлежащий уровень информационной безопасности, одного из показателей конкурентоспособности организации.

Ключевые слова: модель обеспечения информационной безопасности, ИТ-инфраструктура, корпоративная информационная система, вуз, информационная безопасность.

Dussekeyev R.M., Mutanov G.M., Mamykova Zh.D.

The role of information security in the development of IT infrastructure and increasing the competitiveness of the university

Currently the education sector is developing extremely rapidly, acquiring new features, it's functional, structural, organizational, ideological and value characteristics are transformed. The dramatic transformation is taking place in higher education. All this creates the problem of finding new sources of increasing the competitiveness of the university. The article is devoted to the role of information security to increase the competitiveness of universities. The level of information security, together with key performance indicators of the work of universities, such as: the quality of the educational process, training of future specialists-graduates, the number and quality of scientific research, highly qualified teaching staff, is an important indicator, since the quality of information security at the university directly affects the reputation and thus its competitiveness. Nowadays, the higher education institutions have not formalized procedures, actions, or measures for the protection of IT infrastructure, there is no a management model of information security.This paper analyzes the main threats to the security of information systems (IS) of higher education institutions, based on the results the management model that can be used as a basis for creating own information security system of universities is proposed.

Using this model will effectively prevent and proactively identify threats to information security of IT infrastructure and ensure an appropriate level of information security, one of the indicators of competitiveness of the organization.
Key words: model of information security provision, IT infrastructure, corporate information system, university, information security.

Дусекеев Р.М., Мұтанов Ғ.М., Мамыкова Ж.Д.

Университеттің IT-инфрақұрылымын дамыту мен бәсекеге қабілеттілігін арттыруында ақпараттық қауіпсіздігінің рөлі

Қазіргі уақытта білім беру секторы жаңа сипаттарды алып, өте тез дамып келеді, оның функционалдық, құрылымдық, ұйымдастырушылық, идеологиялық және құндылықты сипаттамалары өзгеріп келеді. Жоғары білім мектебінде өте маңызды трансформациялар болып жатыр. Осының барлығы университеттің бәсекеге қабілеттілігін арттыру үшін жаңа көздерін табу мәселесін тудырады.Мақала жоғары оқу орындарының бәсекеге қабілеттілігін арттыру үшін ақпараттық қауіпсіздіктің (АҚ) рөліне арналған. АҚ деңгейі, университеттердің жұмысының тиімділігінің негізгі көрсеткіштері: білім беру үдерісінің сапасы, болашақ мамандар-түлектерінің дайындығы, ғылыми зерттеулердің саны мен сапасы, жоғары білікті профессор-оқытушылар құрамымен бірге маңызды көрсеткіш болып табылады, өйткені жоғары оқу орында ақпараттық қауіпсіздікті қамтамасыз ету сапасы, оның беделіне және, осылайша, бәсекеге қабілеттілігіне тікелей әсер етеді. Бүгінгі күні, жоғары оқу орындарында АТ-инфрақұрылымды қорғау үшін нысандандырылған рәсімдер, іс-әрекеттер немесе шаралар және ақпараттық қауіпсіздікті басқару моделі жоқ. Бұл еңбекте жоғары оқу орындарының ақпараттық жүйелердің (АЖ) қауіпсіздігі үшін негізгі қауіп-қатерлеріне талдау жасалған, оның нәтижелері негізінде жоғары оқу орындарының өз ақпараттық қауіпсіздік жүйесін құру үшін негіз ретінде пайдалануға болатын басқару моделі ұсынылады. Осы модельді пайдалануы АТ-инфрақұрылымының ақпараттық қауіпсіздігі үшін қатерлерін тиімді алдын алуға және алдын-ала анықтауға мүмкіндік береді және ұйымның бәсекеге қабілеттілігін көрсеткіштерінің бірі, ақпараттық қауіпсіздіктің тиісті деңгейін қамтамасыз етеді.
Түйін сөздер: ақпараттық қауіпсіздікті қамтамасыз ету моделі, АТ-инфрақұрылым, корпоративтік ақпараттық жүйесі, ЖОО, ақпараттық қауіпсіздік.

1 Введение

Вуз обладает рядом особенностей, связанных с многопрофильным характером деятельности, множеством форм и методов учебной работы, наличием развитой структуры вспомогательных подразделений и служб, отсутствием общепринятой формализации деловых процессов, необходимостью электронного взаимодействия с вышестоящими организациями, частым изменением статуса сотрудников и обучаемых, многообразием источников финансирования, пространственной распределенностью инфраструктуры [1]. Мы видим, что вуз – это самостоятельная организация, которая оказывает образовательные услуги с целью подготовки высококвалифицированных и востребованных кадров для экономики страны. В этой связи для вуза является важным наличие такого качества, как конкурентоспособность, чтобы быть привлекательным и интересным для научных деятелей и будущих студентов. Важными показателями конкурентоспособности университета являются качество образовательного процесса, подготовка будущих специалистов-выпускников, количество и качество научных исследований, высококвалифицированный профессорско-преподавательский состав, инфраструктура [2]. В связи с отсутствием формализации бизнес-процессов менее заметным остается такой показатель, как уровень информационной безопасности высшего образовательного учрежде-

ния. Тем не менее, данный показатель является особенно важным, так как качество обеспечения информационной безопасности в вузе непосредственно влияет на репутацию и соответственно на его конкурентоспособность. В университете, как часть непрерывного процесса оказания образовательных услуг, хранится и обрабатывается огромное количество различных данных, связанных не только с обеспечением учебного процесса, но и с научно-исследовательскими и проектно-конструкторскими разработками, персональные данные студентов и сотрудников, служебная, коммерческая и иная конфиденциальная информация. Мы видим, что университет обладает большим количеством информации, использование и обеспечение безопасности которой регламентируется действующими законодательными актами. Таким образом, обеспечение надлежащего уровня информационной безопасности университета в связи с положениями Закона РК от 21 мая 2013 года № 94-V "О персональных данных и их защите" , Закона РК от 27 июля 2007 года № 319-III "Об образовании" и Закона РК от 24 ноября 2015 года № 418-V "Об информатизации" также становится актуальной задачей.

На основании выше изложенного мы пришли к выводу, что для университета необходимо сформировать бизнес-процесс обеспечения информационной безопасности посредством разработки нормативно-регламентирующих документов и контролирующих мер.

2 Текущее состояние ИТ-инфраструктуры вуза и базовая модель обеспечения информационной безопасности

Для построения базовой модели обеспечения информационной безопасности необходимо определить компоненты ИТ-инфраструктуры вуза и выделить среди них объекты информационной безопасности, определить угрозы, а также определить основные проблемы, препятствующие реализации данной базовой модели.

Мы видим, что компонентами ИТ-инфраструктуры практически любого высшего учебного заведения являются определённое аппаратное и программное обеспечение [3].

К аппаратному обеспечению относится:

Сетевая инфраструктура – состоит из системно-коммуникационных узлов сети; структурированной кабельной системы; активного сетевого оборудования; IP-телефонии; локального IP-телевидения; системы управления, контроля и мониторинга безопасности сети.

Серверная инфраструктура – включает в себя: сервера; системы хранения данных; вычислительные системы научных расчетов; системы резервного копирования и восстановления; средства виртуализации; системы администрирования вычислительных системных ресурсов и сервисов; систему гарантированного электропитания; систему контроля и мониторинга окружающей среды; систему пожаротушения.

Мультимедийное технико-технологическое обеспечение – это парк компьютерной техники и оргтехники; интерактивное мультимедийное оборудование; система видеоконференцсвязи; аппаратные средства мобильного обучения; система аудио-видео сопровождения; учебное программное обеспечение.

К программному обеспечению относится:

Корпоративная информационная система управления вузом (КИС) – представляет собой комплекс программ, направленных на автоматизацию и управление различными

бизнес-процессами вуза, базирующихся на процессном подходе, что позволяет системно развивать каждое направление деятельности вуза и организовывать работы по созданию и сопровождению программных разработок работниками информационных подразделений вуза.

Корпоративная информационная система управления вузом содержит следующие категории информации, подлежащие защите:

1) информация, содержащая персональные данные работников, обучающихся вуза.

2) информация, содержащая коммерческую тайну.

3) информация, предназначенная для конкретных лиц, либо группы лиц, с ограниченным доступом.

Как видно из описания компонентов ИТ-инфраструктуры, каждый из них представляет собой объект информационной безопасности. Следовательно, нужно по каждому объекту определить угрозы, процедуру организации и систему мер по обеспечению информационной безопасности.

Первоисточниками угроз информационной безопасности являются интернет и интранет среды. В соответствии с рисунком 1 мы видим категории угроз со стороны интернет и интранет.

К основным угрозам, исходящим из обозначенных на рисунке 1 источников, можно отнести следующие:

– внедрение вирусов и других разрушающих программных воздействий;

– нарушение целостности исполняемых файлов;

– использование ошибок кода и конфигурации программного обеспечения (ПО), активного сетевого оборудования;

– анализ и модификация ПО;

– наблюдение за работой системы путем использования программных средств анализа сетевого трафика и утилит операционных систем (ОС), позволяющих получать информацию о системе и о состоянии сетевых соединений;

– использование уязвимостей ПО для взлома программной защиты с целью получения несанкционированного доступа к информационным ресурсам или нарушения их доступности;

– выполнение одним пользователем несанкционированных действий от имени другого пользователя;

– раскрытие, перехват и хищение секретных кодов и паролей;

– чтение остаточной информации в оперативной памяти (ОП) компьютеров и на внешних носителях;

– загрузка и установка в системе не лицензионного, непроверенного системного и прикладного ПО;

– блокирование работы пользователей системы программными средствами;

– перехват информации на линиях связи путем использования различных видов анализаторов сетевого трафика;

– замена, вставка, удаление или изменение данных пользователей в информационном потоке;

– перехват информации (например, пользовательских паролей), передаваемой по каналам связи, с целью ее последующего использования для обхода средств сетевой аутентификации;

– статистический анализ сетевого трафика (например, наличие или отсутствие определенной информации, частота передачи, направление, типы данных и т.п.);

– размещение конфиденциальной/провокационной информации в сети Интернет;

– атаки типа "отказ в обслуживании" (DoS) т. е. атаки на вычислительную систему с целью довести её до отказа, создание таких условий, при которых добросовестные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднён;

– кража важных данных с помощью карманных носителей информации (flash-накопителей, внешних жестких дисков и т. д.);

– фишинг, т. е. интернет мошенничество с использованием социальной инженерии для получения доступа к конфиденциальной информации пользователей – логинам и паролям;

– низкая квалификация ИТ-специалистов, администраторов и разработчиков программного и технического обеспечения;

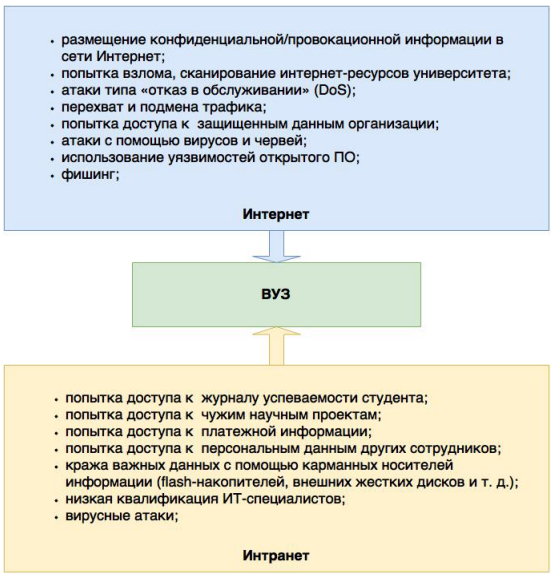

Рисунок 1 – Схема возможных угроз ИБ для вуза

Из анализа угроз информационной безопасности можно сделать вывод, что в вузе присутствует ряд проблем, препятствующих реализации процедуры организации и системы мер по обеспечению информационной безопасности:

1) отсутствие или недостаток специалистов ИБ в вузе;

2) дороговизна средств мониторинга и диагностики сетевого, серверного и программного обеспечения;

3) отсутствие общепринятой формализации деловых процессов, в том числе процессов по обеспечению информационной безопасности;

4) реагирование по факту произошедшего инцидента информационной безопасности и отсутствие упреждающих действий по предотвращению угроз.

Определив объекты, угрозы, а также проблемы информационной безопасности, как практическую часть реализации базовой модели информационной безопасности, необходимо использовать основной набор защитных инструментов, среди них:

Средства авторизации – предоставление определённому лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий. Часто можно услышать выражение, что какой-то человек "авторизован"для выполнения данной операции – это значит, что он имеет на неё право.

Журналирование – процесс записи информации о происходящих с каким-то объектом (или в рамках какого-то процесса) событиях в журнал / лог-файл (например, в файл).

Антивирусные средства – специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления заражённых (модифицированных) такими программами файлов, а также для профилактики – предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Межсетевые экраны – программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами.

Системы резервного копирования – процесс создания копии данных на носителе, предназначенном для восстановления данных в оригинальном или новом месте их расположения в случае их повреждения или разрушения.

Системы бесперебойного питания – вторичный источник электропитания, предназначенный для электропитания при кратковременном отключении основного источника электропитания, а также для защиты от существующих помех в сети с сохранением допустимых параметров для сети основного источника.

Системы аутентификации – средство защиты, устанавливающее подлинность лица, получающего доступ к автоматизированной системе, путем сопоставления сообщенного им идентификатора и предъявленного подтверждающего фактора.

Средства контроля доступа в помещения – совокупность программно-аппаратных технических средств безопасности, имеющих целью ограничение и регистрацию входа-выхода объектов (людей, транспорта) на заданной территории через "точки прохода": двери, ворота, КПП.

3 Управляющая модель обеспечения информационной безопасности

Для обеспечения более высокого и качественного уровня защиты объектов ИТ-инфраструктуры от вышеуказанных угроз образовательная организация должна уметь руководствоваться существующими законодательными документами об информационной безопасности, а также обладать исчерпывающими организационными положениями касательно процедур обеспечения информационной безопасности. Нормативные регламентирующие документы должны содержать конкретные программно-технические решения общие для всех образовательных учреждений с учетом их особенностей в защите информации.

На сегодняшний день в учреждениях высшего образования отсутствует формализованные процедуры, действия или меры по защите ИТ-инфраструктуры. Таким образом университеты не обладают формализованной управляющей моделью обеспечения информационной безопасности.

В связи с вышеизложенным мы видим необходимость создания управляющей модели обеспечения информационной безопасности, которая будет состоять из вышеописанной базовой модели и дополнительных мер, и процедур, описанных ниже:

Шаг 1. Определение объектов информационной безопасности.

1.1 Определение объектов защиты ИТ-инфраструктуры - анализ и выявление ценных информационных объектов, например, конфиденциальные данные организации, серверные, сетевые и информационные ресурсы и т.д. Эти объекты защиты будут использованы для определения угроз, которые могут нанести ущерб данным объектам.

1.2 Определение угроз информационной безопасности ИТ-инфраструктуры – анализ и выявление потенциально возможных событий, действий, процессов или явлений, которые могут привести к нанесению ущерба. Для определения угроз необходимо оценить имеющиеся уязвимости, т. е. присущие объекту ИТ-инфраструктуры причины, приводящие к нарушению информационной безопасности. Определив угрозы, можно точно понять и определить, каких последствий от них ожидать в случае их реализации.

1.3 Определение последствий реализации угроз – анализ и выявление возможных действий реализации угрозы при взаимодействии источника угрозы через имеющиеся уязвимости. После определения последствий будет сформирована вся цепочка объектов информационной безопасности, которую можно использовать, как входные данные для составления организационных процедур информационной безопасности.

Шаг 2. Организация процедур информационной безопасности.

2.1 Формирование матрицы доступа к объектам ИТ-инфраструктуры (серверные, сетевые и информационные ресурсы) – таблицы, отображающей правила доступа субъектов к объектам ИТ-инфраструктуры, данные о которых хранятся в диспетчере доступа. Определив соответствующую матрицу, доступ необходимо каким-то образом физически разграничить. Для этой и других целей нужно использовать защитные инструменты.

2.2 Использование базового набора защитных инструментов – программно-технических способов и средств обеспечения информационной безопасности. В итоге будет создана базовая модель обеспечения информационной безопасности. Но мало просто использовать данную модель, нужно контролировать правильность и эффективность ее использования и производить мониторинг состояния информационной безопасности.

Шаг 3. Реализация и внедрение мер, выработка решений мониторинга и контроля информационной безопасности.

3.1 Формирование набора нормативных документов – документов, содержащих положения относительно обеспечения информационной безопасности, созданных и регулируемых как самой организацией, так и государством. Создав такой набор документов можно определить меры и конкретные, выражаемые в числах, показатели информационной безопасности.

3.2 Определение показателей оценки информационной безопасности – например, это могут быть количество вирусов, обнаруженных за месяц, количество попыток загрузки вредоносных файлов на сервер через сайты организации, сроки окончания лицензий различных ПО, количество одновременных пользователей на сайте в среднем каждый день, число сбоев, когда внутренние системы и сайты организации останавливали свою работу, данные конфигурации баз данных и серверов, данные о загруженности центрального процессора серверов, количество новых персональных компьютеров (ПК) без установленных программ обеспечения безопасности. Данные показатели должны быть

отражены в соответствующих протоколах принятия решений при преодолении последствий случившихся инцидентов и использоваться для принятия решений при планировании модернизации ИТ-инфраструктуры, например, покупки дополнительных средств защиты, а также при выработке каких-либо упреждающих действий по защите. По данным показателям возможно и желательно построить ИС мониторинга, к которой будут иметь доступ руководство ИТ-подразделения для того, чтобы оперативно принимать решение о состоянии информационной безопасности ИТ-инфраструктуры вуза.

4 Заключение

В связи с вышеизложенным нами разработана управляющая модель обеспечения информационной безопасности для вузов, состоящая из следующих компонентов – это нормативно-регламентирующие документы, системы мониторинга, анализа и контроля, набор показателей оценки информационной безопасности.

Использование такой модели позволит эффективно предупреждать и заранее выявлять угрозы информационной безопасности ИТ-инфраструктуры, и своевременно информировать руководство вуза о текущем состоянии программно-технического комплекса, и понимать его уровень защищенности, и оценить надёжность его защиты.

Таким образом, реализация вышеописанной модели позволит подтвердить, что вузом, в частности его руководством, приняты все необходимые меры по обеспечению надлежащего уровня информационной безопасности, и способствовать устойчивому развитию конкурентоспособности вуза.

Литература

[1] *Проталинский О.М., Ажмухамедов И.М.* Информационная безопасность вуза // Вестник Астраханского государственного технического университета. Сер. Управление, вычислительная техника и информатика. – 2009. – № 1. – С.18-23.

[2] *Белоусова Е.В., Савченко И.И.* Особенности оценки конкурентоспособности вуза на рынке образовательных услуг // Известия Дальневосточного федерального университета. Экономика и управление. – 2006. – № 1. – С.11-18.

[3] *Иванов И.П.* IT-инфраструктура современного университета // Science Time. - 2015. – № 2(14). – С.53-56.

References

[1] *Protalinskiy O.M., Azhmuhamedov I.M.* Information security of institute of higher education // Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics. – 2009. – No 1. – P.18-23.

[2] *Belousova E.V., Savchenko I.I.* Features of university competitiveness assessment in the market of educational services // Izvestia of Far Eastern Federal University. Economics and Management. – 2006. – No 1. – P.11-18.

[3] *Ivanov I.P.* IT-infrastructure of the modern university // Science Time. – 2015. – No 2(14). – P.53-56.