ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ВЫСШЕГО УЧЕБНОГО ЗАВЕДЕНИЯ В РАМКАХ СОВРЕМЕННОЙ ГЛОБАЛИЗАЦИИ

Литвинов В.А., Лыпко Е.В., Яковлева А.А.
Оренбургский государственный университет, г. Оренбург

Аннотация: дать определение и характеристику глобализации, роль информационной безопасности в ВУЗе.
Ключевые понятия: глобализация, национальная безопасность, корпоративная сеть ВУЗа, информационная безопасность.

Согласно Большому толковому словарю русского языка Кузнецова С.А., глобализация – это широкое распространение влияния какого-либо процесса, явления за пределы какой-либо страны или за пределы какого-либо вида деятельности. Мы согласны с данным мнением, так как в настоящее время процесс глобализации рассматривается в контексте национальной безопасности страны. В настоящее время в мире происходит процесс глобализации, который определяет будущее развитие человечества, целенаправленно и непосредственно влияет на национальную безопасность страны, на мировое сообщество, в целом. В настоящее время Российская Федерация столкнулась с данной проблемой, а именно: в современных условиях всеобщей информатизации и развития информационных технологий усиливаются угрозы национальной безопасности нашей страны в информационной сфере.
Указ Президента РФ "О Стратегии национальной безопасности Российской Федерации" гласит, что национальная безопасность Российской Федерации - состояние защищенности личности, общества и государства от внутренних и внешних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан Российской Федерации, достойные качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие Российской Федерации. Национальная безопасность включает в себя оборону страны и все виды безопасности, предусмотренные Конституцией Российской Федерации и законодательством Российской Федерации, прежде всего государственную, общественную, информационную, экологическую, экономическую, транспортную, энергетическую безопасность, безопасность личности. Национальной безопасность РФ применима к информационной сфере, которую развивает Доктрина информационной безопасности Российской Федерации: обеспечение информационной безопасности РФ играет ключевую роль в обеспечении национальной безопасности РФ. При этом одним из приоритетных направлений государственной политики в области обеспечения информационной безопасности РФ является совершенствование подготовки кадров, развитие образования в области информационной безопасности. Особую роль в решении этих задач играют ВУЗы.

В современном ВУЗе 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.

Рост количества преступлений в сфере информационных технологий с каждым годом растет. Встала задача разработки интегрированной системы безопасности.

Информационная безопасность ВУЗа будет эффективна, если:

- будут грамотно и четко сформулированы цели, задачи, принципы и ключевые направления обеспечения информационной безопасности;
- разработаны сценарии необходимости и значимости баланса в информационной
открытости и конфиденциальности;
- определены роли и места политики информационной безопасности в управлении
информационными ресурсами ВУЗа и выработаны согласующиеся принципы и подходы;
- разработаны базовые методики управления процессом обеспечения политики информационной безопасности;
- подготовлены проекты нормативно-правовых документов.

Вышеперечисленные элементы определяют единую политику обеспечения безопасности информации в ВУЗе. Специфика защиты информации в образовательной системе заключается в том, что ВУЗ – заведение с огромным количеством участников образовательного процесса, а также место повышенной активности «начинающих киберпреступников». К киберпреступникам относятся студенты, возраст которых 18-23 года. Что же движет этими людьми? Желания стать популярным среди ровесников? Нанести урон информационной безопасности ВУЗа? Скорее всего, юными «вундеркиндами» движет сильнейшее желание быть в кругу внимания, стать популярным среди своих сверстников, создать «вирус», «наказать» преподавателя, заблокировать выход в сеть Интернет, подкорректировать свои оценки и т.д. Первый преступник в области информационной безопасности был студент ВУЗа – червь Морриса, который заразил несколько ЭВМ копиями таинственной программы.

Современные ВУЗы, как объекты информатизации, имеют ряд особенностей. К ним можно отнести: разнопрофильный характер деятельности, наличие пространственной инфраструктуры (филиалы, представительства), многообразие форм и методов учебной работы, адаптация к постоянно меняющимся условиям образовательного рынка, электронное взаимодействие с юридическими организациями, периодическая смена статуса преподавателей и студентов.

Данные особенности требуют соблюдения следующих требований:

- применение надежных технологий, обеспечивающих высокий уровень информационной безопасности;
- разработка документации на базе рационального применения стандартов, что обуславливает создание успешной системы;
- использование модульной структуры приложений, где каждый модуль отвечает за определенную группу деловых процедур;
- привлечение большого числа профессиональных специалистов, компетентных в обеспечении информационной безопасности.

Масштабное внедрение Интернета и различного рода информационных установок в образовательный процесс привело к появлению корпоративных сетей. Корпоративная сеть ВУЗа – это информационная система, содержащая компьютеры, серверы, сетевое оборудование, средства связи и телекоммуникации, систему программного обеспечения, предназначенную для решения задач управления ВУЗом и ведения образовательной деятельности.

Мы проанализировали информационную безопасность корпоративных сетей ВУЗов и выделили рад следующих проблем:

1. «Скудное финансирование» касаемо оборудования, кадров и нелицензионного программного обеспечения.
2. Корпоративные сети не имеют стратегических целей развития. Программное обеспечение рассматривается исключительно с позиций текущих задач.
3. Одновременно в одной сети работает несколько информационных систем или подсистем управления (АСУ «Студент, АСУ «Учебный процесс», АСУ «Библиотека», АСУ «Кадры» и т.д.)
4. Планы комплексной информационной безопасности либо отсутствуют либо не соответствуют современным запросам.

При наличии вышеперечисленных проблем в корпоративных сетях возможны следующие угрозы, как внутренние, так и внешние, информационной безопасности:
- удаление информации из библиотек;
- попытка взлома АСУ «ВУЗ»;
- запуск игровых программ;
- установка вирусных программ и троянских коней;
- сканирование сетей через Интернет;
- несанкционированный запуск программ;
- попытки проникновения в системы бухгалтерского учета;
- несанкционированная откачка из Интернета нелицензионного программного обеспечения и т.п.

В связи с этим мы предлагаем следующие рубежи защиты информационных сетей ВУЗа. Во-первых, чтобы исключить риски, связанные с утечкой и порчей информации, корпоративные сети не должны подключаться к глобальным сетям и общей университетской сети. Как правило, связь с Интернетом осуществляется сразу по нескольким линиям связи (оптоволоконная магистраль, спутниковые и радиоканалы). Отдельные каналы предоставляются

для связи с другими ВУЗами и для безопасного обмена данными. Поэтому особенно важные узлы для обмена данными (к примеру, бухгалтерия) должны существовать отдельно.

Во-вторых, для обороны от атак извне (Интернет) необходимо применять роутер (маршрутизатор). Он позволяет связать участки сети друг с другом, рационально разделить трафик и использовать альтернативные пути между узлами сети. От настроек роутера будет зависеть функционирование подсетей и связь с глобальными сетями. Главная задача маршрутизатора в плане безопасности – защита от атак.

Следующий рубеж защиты мы связываем с прокси-сервером, который обрабатывает запросы от рабочих станций учебного персонала, серверов, не подключенных напрямую к роутеру, и фильтрует трафик. На этом уровне особенно важно экономить трафик (блокировка страниц нецензурного содержания, фильтрация мультимедиконтента). На данном сервере обязательно размещать антивирусные средства. На почтовом же сервере оправдано размещение почтового антивируса. Так же некоторые ВУЗы имеют свой пул дозвона для выхода в Интернет и используют каналы связи учреждения. Во избежание использования данного доступа посторонними лицами в незаконных целях кадровый состав учебного заведения не должен разглашать телефон пула, логин и пароль.

В-четвертых, это финансовая политика развертывания, развития и поддержания в актуальном состоянии корпоративной сети ВУЗа. В-пятых, улучшение кадрового состава информационного центра. Данная политика предполагает привлечение опытных сисадминов к работе. И наконец, это формирование морально-этических норм толерантного поведения в информационных системах и адекватного ограничения от посещений агрессивных информационных пространств.

Таким образом, проблема обеспечения национальной безопасности в современном мире приобретает особую актуальность, что напрямую связано с последствиями процесса глобализации. Глобализация, являющаяся доминирующей тенденцией современного мирового общества, , также влечет за собой и новые риски, вызовы и опасности. Степень защищенности сетей и сервер большинства ВУЗов России оставляет желать лучшего. Одна из приоритетных причин этому – недостаточная организация мер по разработке и обеспечению политики информационной безопасности и недооценка важности данных мероприятий. Немаловажной причиной выступает и недостаточное финансирование закупок оборудования и внедрения новых технологий в сфере информационной безопасности.

Список литературы:

1. *Концепция национальной безопасности РФ, утверждена Указом Президента РФ от 17.12.97 г. № 1300 (в ред. Указа Президента РФ от 10.01.2000 г. № 24).*

2. *Доктрина информационной безопасности Российской Федерации, утверждена Президентом РФ 9.09.2000 г. Пр-1895.*

3. *Проталинский, О.М. Информационная безопасность ВУЗа/ Проталинский О.М., Ажмухамедов, А.М.// Вестник АГТУ. Сер.Управление, вычислительная техника и информатика. – 2009. -№1. – С.18-23. - ISSN 2072-9502.*

4. *Волох, О.В. Глобализация: угроза и вызовдля национальной безопасности России/ Волох О.В., Васильева Н.Н.// Вестник Омского университета. - 2012. - № 3. - С. 306–310.*

5. *Труфанов, А. И. Политика информационной безопасности вуза как предмет исследования [Электронный ресурс]/ Труфанов, А.И. // Проблемы Земной цивилизации. – Вып. 9. – Иркутск: ИрГТУ, 2004. – Режим доступа: library.istu.edu/civ/default.htm.*

6. *Волков, А. В. Обеспечение ИБ в вузах [Электронный ресурс]/ Волков, А.В.// Информационная безопасность. – 2006. – № 3, 4. – Режим доступа: http://www.itsec.ru/articles2/bepub/insec–3 + 4–2006.*

7. *Крюков, В. В. Реализация корпоративной вычислительной сети вуза на базе технологии Active Directory/ Крюков В.В., Майоров В.С., Шахгельдян К.И. // Тр. Всерос. науч. конф. «Научный сервис в сети Интернет». – Новороссийск, 2002. – С. 253–255.*