Среди перечисленных стандартом де-факто выступает NetPolice, бесплатный вариант которой не пропускает только категории, связанные с насилием, алкоголем, и наркотиками. На практике зачастую требуется более серьезная фильтрация, чем та, которую обеспечивают начальные настройки. Следует отметить, что бесплатная версия этого продукта под Windows не настраивается, а работа в Linux-среде подразумевает хорошее знание категорий и настроек.

Таким образом, в настоящее время существует ряд программных средств контент-фильтрации, обладающих различной степенью интеллекта, стоимостью, легкостью в настройке и качестве фильтрации. Выбор конкретного продукта обусловлен особенностью образовательной среды.

Библиографический список

1. *Прохоров А*. «Приличный» Интернет в школе и дома. – КомпьютерПресс. – №2. 2007. – Режим доступа: http://www.compress.ru/article.aspx?id=17262&iid=799 (Проверено 16.02.2013)
2. *Уваров А.С.* Ubuntu Server. Настраиваем контент-фильтр роутера (DansGuardian). – Режим доступа: http://interface31.ru/tech_it/2010/03/ubuntu-server-nastraivaem-kontent-fil-tr-routera-dansguardian.html
3. http://www.icensor.ru/
4. http://www.netpolice.ru/
5. http://skf.edu.ru/

О.А. Матвиенко, Т.Н. Виноградова, П.Н. Матвиенко

ОСНОВНЫЕ АСПЕКТЫ ФОРМИРОВАНИЯ КОНЦЕПЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОРГАНИЗАЦИИ ДИСТАНЦИОННОГО ОБУЧЕНИЯ

ra9mlo@mail.ru, vintani@mail.ru
Омский государственный технический университет

This article is about organization of distance learning. In this case you should pay special attention on the problem of support of the information security at data transmission. This article answers to the main questions of information security at data transmission.

В настоящее время актуальной темой для обсуждения становится обеспечение информационной безопасности в вузе. Количество угроз постоянно растет, что приводит к необходимости изменения методов и способов обеспечения учебного процесса. Невозможно в системе высшего профессионального образования обойтись без применения информационных технологий, которые используются, как в самом образовательном процессе, хранении информации, так и для передачи информации от преподавателя к студенту. Необходимо отметить, что последнее время в вузах развита система интернет-тестирования, а также повсеместно внедряются и используются современные дистанционные технологии обучения студентов заочников. Любое вмешательство в информационную систему может привести к нежелательным последствиям, которые скажутся на качестве образовательного процесса в целом.

С точки зрения обеспечения информационной безопасности, вуз отличается рядом таких особенностей, как:

- огромный поток информации, циркулирующей в информационной среде;
- большие территории, которые занимает вуз;

- большое скопление людей, основная масса из которых студенты – молодые люди в возрасте от 18 до 23 лет, а с точки зрения защиты информации именно эта категория людей является наиболее уязвимой;
- наличие в информационной среде различных наработок в области научной деятельности, представляющих собой интеллектуальную собственность и т.д.

Вышеперечисленные особенности приводят к неконтролируемому росту количества уязвимостей, увеличению числа угроз со стороны внешних и внутренних злоумышленников и, соответственно, трудно предсказуемым потенциальным материальным, финансовым, моральным и другим видам потерь.

Особое внимание необходимо уделить организации дистанционного обучения. На сегодняшний день существует ряд угроз и рисков, борьба с которыми будет способствовать не только эффективному обеспечению информационной безопасности, но и организации качественного и конкурентоспособного процесса в дистанционном обучении. По мнению Зуева В.Е., можно выделить следующие типичные угрозы нормальному функционированию системы электронного обучения:

- неавторизованный доступ к цифровому контенту, включая физический доступ к серверам;
- нарушение целостности и неадекватность учебных ресурсов (часто электронные учебные пособия, наряду с ресурсами Интернета, являются основными источниками учебной информации для студента);
- нарушение безопасности процедур тестирования и электронных экзаменов (проблемы идентификации студентов, списывания, плагиата и адекватного функционирования системы оценивания знаний);
- нарушение нормального функционирования служб и сервисов учебного заведения.[3]

Отсюда можно выделить основные сервисы безопасности, которые должны применяться для построения полноценной системы защиты информационной среды и организации дистанционного образования:

- конфиденциальность;
- аутентификация;
- целостность;
- невозможность отказа;
- контроль доступа;
- доступность.

Данные сервисы реализуются механизмами безопасности, а именно алгоритмами симметричного, асимметричного шифрования и хэш-функциями.

Вторым немаловажным вопросом является обеспечение безопасности некоторой информационной системы, к которой необходимо предотвратить нежелательный доступ или настроить временной доступ с четким указанием периодов.

В данном случае следует руководствоваться сервисами безопасности, которые условно можно разбить на две линии защиты:

- Первая линия, так называемая «сторожевая», направленная на предотвращение атак (различные межсетевые экраны);

- Вторая линия состоит из разнообразных внутренних мониторов, контролирующих доступ и анализирующих деятельность пользователей уже допущенных в защищенную информационную среду пользователей.

При использовании данных сервисов и механизмов существует момент, когда аутентификация с помощью пароля или общего секрета защищает двух или более участников взаимодействующих в защищаемой информационной среде от нарушителей, но не защищает от нарушения осуществляемого друг перед другом (как вариант нарушения – использование чужих научных трудов). В этой ситуации необходимо применить более действенный способ, чем аутентификация на основе общего секрета. Как вариант решения данной проблемы можно предложить использование электронно-цифровой подписи.

Данная подпись должна обладать обязательными свойствами такими как:

- ЭЦП должна использовать уникальную информацию отправителя;
- ЭЦП должна зависеть от сообщения, которое она заверяет;
- ЭЦП должна легко генерироваться и проверяться.

Значительное увеличение за последние годы применяемых информационных технологий в деятельности вуза и, как следствие, расширение информационного пространства должны существенно расширить методы и способы, регулирующие вопросы информационной безопасности. Оптимальным решением вопроса при создании защищенной информационной среды вуза и организации дистанционного образования является использование удостоверяющих центров, обеспечивающих посредством электронно-цифровой подписи и защищенных каналов связи решение задач по обеспечению должного уровня безопасности.

Библиографический список

1. *Васильев В.И., Савина И.А., Шарипова И.И.* «Построение нечетких когнективных карт для анализа и управления информационными рисками вуза»/ Вестник ИГАТУ, т.10, № 2(27), с. 199-209

2. *Зуев В.Е.* «Безопасность электронного обучения», Международная конференция "Информационные технологии в образовании" "ИТО-Москва-2010".

Л.Ю. Овсяницкая

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК КЛЮЧЕВОЙ ВОПРОС ПОДГОТОВКИ СПЕЦИАЛИСТОВ ЗДРАВООХРАНЕНИЯ К РАБОТЕ В УСЛОВИЯХ ФОРМИРОВАНИЯ ЕДИНОЙ ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СРЕДЫ

larovs@rambler.ru

Уральский социально-экономический институт (филиал) ОУП ВПО «АТиСО», г. Челябинск

The article focuses on information security problems that need to pay attention during the computer science postgraduate medical education. The obtained knowledge will allow the doctors to use the advantages of the unified state information environment and to protect confidential personal and business information from the illegal distribution.

В 2011 г. утверждена Концепция создания единой государственной информационной системы в сфере здравоохранения. Основной целью создания системы является повышение качества оказания медицинской помощи на основе совершенствования информационно-технологического обеспечения медицинских и фармацевтических организаций.

Все данные о состоянии здоровья граждан России относятся к числу конфиденциальных. Защита персональных данных граждан в единой системе обеспечивается использованием