того, персональный ЭДП обеспечивает автоматическое формирование обязательных отчетных документов практики, а именно:

1. Задание на практику;
2. Дневник практики;
3. Итоговый отчет практики;
4. Отзыв руководителя от предприятия,

при условии регулярной и методичной работы

Библиографический список

1. Элетронный дневник практики (серверная часть). http://diplom.16mb.com, http://diplom.susu.ac.ru

2. Online manual for WordPress and a living repository for WordPress information and documentationonline manual for WordPress and a living repository for WordPress information and documentation. http://codex.wordpress.org/

В.Б. Лапшина, В.Н. Макашова

ОСНОВЫ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ

vlapshina@masu-inform.ru, vmakashova@masu-inform.ru
ФГБОУ ВПО «Магнитогорский государственный университет», г. Магнитогорск

In article questions of the organization and carrying out of audit of information security of educational institution are considered. The basic stages and results of audit are resulted.

Обеспечение информационной безопасности (ИБ) в условиях информатизации образования становится одной из приоритетных задач в деятельности образовательного учреждения. Обеспечение информационной безопасности осуществляется по следующим направлениям:

- правовая защита – это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;
- организационная защита – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба;
- техническая защита – это использование различных технических средств, препятствующих нанесению ущерба.

Управление информационной безопасностью – это сложный, многоаспектный процесс, включающий: разработку стратегии ИБ, аудит, построение системы управления ИБ, мониторинг. Информационная безопасность образовательного учреждения должно соответствовать действующим законодательным актам и нормативным документам Российской Федерации по обеспечению ИБ. Перечислим основные из них: Конституция Российской Федерации, Федеральный закон от 19.12.2005 №160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных», Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных», Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», постановление Правительства Российской Федерации

от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

При построении системы информационной безопасности образовательного учреждения решающую роль играет аудит. Аудит информационной безопасности представляет собой всестороннее обследование, позволяющее оценить текущее состояние информационной безопасности организации и спланировать дальнейшие шаги по повышению уровня защищенности. Аудит информационной безопасности может быть как внутренний, так и внешний. Внутренний аудит направлен на выявление уязвимых мест ИБ, возможных каналов утечки информации и, в целом, позволяет объективно оценить уровень информационной безопасности. Целью внешнего аудита является проверка функционирующей системы управления ИБ образовательного учреждения на соответствие требованиям нормативных документов. Также выделяют следующие виды аудита ИБ: экспертный аудит, тест на проникновение, аудит web-безопасности, аудит информационных систем, комплексный аудит, подготовка к сертификации на ISO.

На наш взгляд, аудит ИБ образовательного учреждения должен включать следующие этапы.

1. Анализ организационно-распорядительных документов образовательного учреждения.

2. Осмотр помещений с точки зрения обеспечения физической безопасности ИТ-инфраструктуры.

3. Анализ средств и технологий защиты информации:

- анализ угроз утечки, хищения, утраты, искажения, подделки информации; угроз безопасности личности, общества, государства;
- анализ угроз несанкционированных действий по уничтожению модификации, искажению, копированию, блокированию информации;
- анализ защиты образовательного учреждения от нежелательного контента в сети Интернет, который может нанести вред их здоровью и развитию.

4. Оценка знаний сотрудников образовательного учреждения в области информационной безопасности.

Результатом аудита информационной безопасности образовательного учреждения является создание документа, который содержит:

- анализ угроз, которые могут быть реализованы, через обнаруженные уязвимости;
- качественная или количественная оценка рисков ИБ;
- оценка соответствия актуальным требованиям;
- рекомендации, которые должны быть выполнены для повышения уровня защищенности образовательного учреждения;
- план реализации разработанных рекомендаций.

На основании результатов аудита ИБ, образовательное учреждение может построить эффективную систему безопасности, минимизировать возможные риски информационной безопасности, что позволит, в будущем, обеспечить родителям, детям и педагогам комфортную и безопасную информационно-образовательную среду.

Исследование выполнено при финансовой поддержке РГНФ в рамках научно-исследовательского проекта РГНФ № 11-06-01006а «Разработка и апробация модели подготовки научно-педагогических кадров к обеспечению информационной безопасности в ИКТ-насыщенной среде».

Библиографический список

1. ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements.
2. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
3. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью
4. BS ISO/IEC 27002:2005 RU Информационные технологии - Методы обеспечения безопасности.
5. ISO/IEC TR 18044:2004 Information technology – Security Techniques – Information security incident management

В.А. Максимов

ПОДДЕРЖАНИЕ УЧЕБНОГО ПРОЦЕССА НА ОСНОВЕ ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ МОМЕНТАЛЬНЫХ СНИМКОВ

v.maximov.mail@gmail.com
Российский государственный профессионально-педагогический университет, Екатеринбург

В учебных заведениях традиционно возникает проблема управления многообразием программных продуктов, применяемым в учебном процессе. Одним из решением данной проблемы является применение технологии виртуализации. Виртуальные машины с установленными программными продуктами распространяются по локальной сети университета на целевые компьютеры клиентов. Важной задачей является уменьшение размера образа виртуальных машин, что напрямую скажется на скорости распространения образов виртуальных машин через локальную сеть, а так же на степень влияния оказываемой на сетевую инфраструктуру университета в период массового развертывания образов.

При работе с виртуальными машинами с использованием подхода «1 приложение = 1 виртуальная машина», помимо преимуществв вопросах безопасности и стабильности становится ярко выраженной высокая стоимость хранения самих образов. Если взять распространённую операционную систему Windows XP в первоначальной установке, то на жестком диске она занимает более 5 ГБ, в будущем к этому числу будет необходимо прибавить размер устанавливаемых приложений. При использовании 10 приложений размер всех виртуальных машин достигает более 50 ГБ. Стоит учитывать, что указанный размер берется без учета пользовательских данных.

Благодаря применению моментальных снимков (снапшотов) с использованием технологии дифференциальных дисков удается сократить используемый размер, убрав из уравнения стоимость веса операционной системы.