Таким образом, с использованием проектной методики разработанная система заданий для обучения родителей в виде серии семинаров на тему: «Родительский контроль: Интернет территория безопасности», будет наилучшим образом способствовать углублению родителей в столь сложную тему. Данный проект поможет внедрить в образовательный процесс работу с родителями, после которой родители научатся обеспечению контроля за ребенком при использовании компьютера и Интернета. Разработанная методика способствует повышению эффективности обучения родителей в области информационной безопасности и может быть рекомендована при обучении родителей детей-подростков.

Публикация выполнена в рамках проекта РГНФ № 11-06-01006 «Разработка и апробация модели подготовки научно-педагогических кадров к обеспечению информационной безопасности в ИКТ-насыщенной среде».

Список литературы

1. *Абулин, К.А.* Безопасность в интернете [Электронный ресурс]. Режим доступа: http://www.comprice.ru/ (дата обращения: 18.03.13*)*.

2. *Белоусова, И.Д.* Введение информационных технологий в процесс обучения студентов вуза [Текст]: монография / И.Д. Белоусова. – Магнитогорск, 2009. – 141 с.

3. Детские браузеры – защита ребенка от угроз интернета [Электронный ресурс]. – Режим доступа: http://www.3dnews.ru/software/detskie_brauzeri/ (дата обращения: 12.01.11).

4. *Змеев, С.И.* Андрагогика и образование взрослых: основные понятия и термины. Понятийный аппарат педагогики и образования [Текст] / С.И. Змеев – Вып. 2. – Екатеринбург, 2002.

5. *Мовчан, И.Н.* Педагогический контроль информационной деятельности студента вуза в процессе профессиональной подготовки [Текст] : автореф. дис. / И.Н Мовчан. – Магнитогорск, 2009. – 24 с.

6. *Мовчан, И.Н.* Проблемы подготовки специалистов в области информационной безопасности [Текст] / И.Н. Мовчан // Открытое образование. – 2013. – № 5. – С. 78-80.

7. Программы контроля, родительский контроль [Электронный ресурс]. – Режим доступа: http://nicekit.ru/parental-control/time-boss.php (дата обращения: 18.05.2013).

8. Социальный сервис «Летописи» [Электронный ресурс]. – Режим доступа: http://letopisi.ru/ (дата обращения: 17.06.13).

УДК 004.00

О.Е. Масленникова

АКТУАЛЬНОСТЬ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ МОДЕРНИЗАЦИИ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Масленникова Ольга Евгеньевна

maslennikovaolga@yandex.ru

ФГБОУ ВПО «Магнитогорский государственный технический университет им. Г.И. Носова», Россия, г. Магнитогорск,

RELEVANCE OF INFORMATION SECURITY IN MODERNIZATION OF CORPORATION INFORMATION SYSTEM

Maslennikova Olga Yevgenievna

Nosov Magnitogorsk State Technical University, Russia, Magnitogorsk

Аннотация . *Рассматриваются ключевые понятия исследования, приводится краткая характеристика стандартов, описание мер и работ по обеспечению информационной безопасности корпоративных информационных систем.*

Abstract. *Discusses the key concepts of research, is a brief description of standards activities and the work of information security of corporate information systems.*

Ключевые слова*: информационная безопасность, корпоративная информационная система, модернизация.*

Keywords*: information security, corporation information system.*

Проблема защищенности информации в корпоративных информационных системах и ее сегментах, регулярный аудит рисков их информационной безопасности и организации в целом определяется как минимум следующим противоречием. С одной стороны вопросы безопасности информационных объектов являются на сегодня широко обсуждаемыми, востребованными в поисках методов и средств их решения, нормативно поддержанными множеством международных и национальных стандартов, кроме того выступают как отдельная сторона финансовых расходов любой организации. С другой стороны, неизменно растут ущербы финансового и материального толка, причиненные собственникам информационных ресурсов от компьютерных атак.

Для однозначного понимания идей рассматриваемого исследования введем несколько понятийных моментов. Во-первых, в данной работе корпоративную информационную систему (КИС) будем определять как информационную систему (ИС) организации, отвечающую следующему минимальному перечню требований: функциональная полнота системы; надежная система защиты информации; наличие инструментальных средств адаптации и сопровождения системы; реализация удаленного доступа и работы в распределенных сетях; обеспечение обмена данными между разработанными ИС и др. программными продуктами, функционирующими в организации; возможность консолидации информации; наличие специальных средств анализа состояния системы в процессе эксплуатации [1].

Во-вторых, согласно стандарту ГОСТ Р ИСО/МЭК 17799-2005, информационная безопасность (ИБ) есть механизм защиты информации, обеспечивающий: конфиденциальность (доступ к информации только авторизованных пользователей); целостность (достоверность и полноту информации и методов ее обработки); доступность (доступ к информации и связанным с ней активам авторизованных пользователей по мере необходимости) [2].

На сегодняшний день нормативно вопросы организации, управления системой ИБ технологий, автоматизированных систем, организации в целом находят отражение в достаточно широком спектре международных и идентичных им национальных стандартах. Перечислим лишь некоторые из них, которые будут полезны для проведения данного исследования (табл.1).

Таблица 1. Назначение стандартов по ИБ, используемых в работе

Название	Назначение
ГОСТ Р ИСО/МЭК 27001-2006 Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования	описывает выстраивание системы ИБ на предприятии; – предъявляет требования не столько к техническим средствам защиты, сколько к системе управления ИБ.
ISO 15408 Часть1-3 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий	часть 1. Введение и общая модель; часть 2. Функциональные требования безопасности; часть 3. Требования доверия к безопасности; предназначен для использования в качестве основы при оценке характеристик безопасности продуктов или систем информационных технологий (ИТ). Устанавливая общую базу критериев, ИСО/МЭК 15408 позволяет сделать результаты оценки безопасности ИТ значимыми для более широкой аудитории
ГОСТ Р ИСО/МЭК ТО 19791-2008 Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем	содержит дополнительные критерии оценки и рекомендации по оценке аспектов безопасности, связанных как с ИТ, так и с применением их в АС; устанавливает: a) определение и модель АС; b) описание расширений концепции оценки безопасности с помощью стандартов серии ИСО/МЭК 15408 необходимых для оценки АС; c) методологию и процесс выполнения оценки безопасности АС; d) дополнительные критерии оценки безопасности, охватывающие те аспекты АС, которые не были представлены критериями оценки безопасности в стандартах серии ИСО/МЭК 15408.

Одним из ключевых вопросов построения системы ИБ в КИС является проблема разработки определенных мер безопасности и обеспечения контроля за их выполнением. Согласно ГОСТ Р ИСО/МЭК ТО 19791 они представлены: управленческими (management controls); организационными (operational controls); техническими (technical controls) [4].

Обеспечение необходимого уровня ИБ КИС требует: a) оценки рисков безопасности применительно к рассматриваемой системе: b) уменьшение рисков для противодействия или устранения рисков безопасности посредством выбора обеспечения безопасности: c) аттестации для подтверждения того, что остаточные риски, являются приемлемыми для системы при дальнейшей ее эксплуатации [4].

Для удобства реализации перечисленных выше мер и этапов работ, будет целесообразным провести параллель со стадиями и этапами создания автоматизированных систем согласно ГОСТ 34.601-90 и определить где и как могут быть представлены требования к ИБ КИС, а на каких этапах – осуществлены. Тем более, что стандарт ГОСТ Р ИСО/МЭК ТО

19791 устанавливает необходимым рассмотрение безопасности в жизненном цикле АС (табл. 2).

Таблица 2. Соответствие работ по обеспечению ИБ АС на всех этапах ее ЖЦ

Стадии	Работы по обеспечению ИБ
Формирование требований к АС	идентификация и оценка рисков для АС; идентификация и оценка остаточных рисков АС; привлечение оценщиков упрощения их ознакомления с системой и ее предполагаемой средой, получения исходных данных;
Разработка концепции АС	запись проекта АС в задание по безопасности АС (ЗБС); определение контрмер обеспечения безопасности самой АС; анализ уязвимости и испытание на проникновение при наличии потенциала нападения, оценка полного ЗБС;
Техническое задание	определение соответствующих параметров конфигурации безопасности
Эскизный проект	создание или приобретение программного обеспечения для систем и бизнес-приложения, включая технические меры безопасности; интеграция и конфигурирование системы, испытание ее разработчиком; создание организационной структуры безопасности, формирование политики, правил и процедур безопасности, интегрирование их в систему;
Технический проект	проверка разработчиком специфических для системы мер обеспечения безопасности (МОБ); внедрение соответствующих параметров конфигурации безопасности; оценка АС;
Рабочая документация	составление отчета о сертификации; подготовка владельцем системы плана корректирующих действий по уменьшению или устранению выявленных уязвимостей; определение аттестующим лицом приемлемости фактических остаточных рисков для функционирования системы; выдача разрешения на эксплуатацию системы как результат стадии сертификации;
Ввод в действие	подготовка и внедрение технических и организационных МОБ; испытание специфических для рабочего места МОБ; повторная проверка др. МОБ; обучение всех задействованных лиц использованию мер и процедур обеспечения безопасности в среде эксплуатации; сбор и оценка записей об эксплуатации технических и организационных МОБ, регистрация журналов аудита и записей мониторинга всего доступа к активам, проверка отсутствия несанкционированных операций и неприемлемых рисков, перевод состояний незащищенности в состояния защищенности в назначенный срок; контроль и оценка наличия проблем с безопасностью изменений, внесенных в ходе регламентного обслуживания; проверка записей о фактическом доступе и использовании активов; своевременное уведомление, проверка и анализ проблем с безопасностью; определение критически важных МОБ АС с целью непрерывного мониторинга их эффективности;
Сопровождение АС	изучение, анализ и тестирование любых предполагаемых или фактических изменений АС, выходящих за рамки регламентного обслуживания; проведение испытаний на проникновение для проверки эффективного функционирования модифицированных мер обеспечения безопасности; предоставление результатов анализа воздействия и испытаний аттестующему лицу для определения необходимости повторной оценки безопасности; проведение (возможно) повторной оценки системы ИБ АС; передача в архив или уничтожение АС после завершения ее эксплуатации; подтверждение аттестующим лицом успешной остановки системы.

Отдельной строкой в проблеме обеспечения ИБ КИС как любой АС стоит оценка уровня ее ИБ. Согласно стандарту ГОСТ Р ИСО/МЭК ТО 19791 этот процесс состоит из следующих этапов: a) определение целей безопасности для АС, которые уменьшат неприемлемые риски до приемлемого уровня; b) выбор и спецификация технических и организационных мер безопасности, которые соответствуют целям безопасности АС, принимая во внимание уже реализованные меры обеспечения безопасности; c) определение конкретных измеримых требований доверия как к техническим, так и организационным мерам обеспечения безопасности, чтобы удостовериться в том, что АС соответствует целям безопасности; d) фиксирование принятых решений в задании по безопасности для АС (ЗБС); e) оценка конкретной АС с тем чтобы сделать вывод о ее соответствии ЗБС; f) периодическая переоценка рисков безопасности АС, так и способности АС противостоять этим рискам.

Выполнение всех обозначенных процессов будет проходить на модернизации КИС образовательного назначения. Все обозначенные положения выполнимы и для такого рода систем.

Список литературы

1. *Назарова, О.Б.* Сопровождение корпоративных информационных систем [Текст] : учебник / О.Б. Назарова, Л.З. Давлеткиреева, О.Е. Масленникова, Н.О. Пролозова. – Магнитогорск : МаГУ, 2013. – 220 с.

2. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью. [Электронный ресурс] – Режим доступа: http://www.rosintelcom.ru/upload/nonormativnaja_basa_zakoni/GOST-17799-2005.pdf (дата обращения: 22.02.2014).

3. ГОСТ 34.601-90 Автоматизированные системы. Стадии создания [Электронный ресурс] – Режим доступа: http://www.prj-exp.ru/gost/gost_34-601-90.php (дата обращения: 22.02.2014).

4. ГОСТ Р ИСО/МЭК ТО 19791 – 2008 Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем [Электронный ресурс]. – Режим доступа: http://standartgost.ru/ (дата обращения: 22.02.2014).

УДК 347.78:004.056

С.В. Ченушкина

МЕТОДЫ БОРЬБЫ С ПЛАГИАТОМ И ЗАЩИТЫ АВТОРСКОГО ПРАВА

Ченушкина Светлана Владимировна

Svch2003@yandex.ru

ФГАОУ ВПО «Российский государственный профессионально-педагогический университет», Россия, г. Екатеринбург

METHODS OF DEALING WITH PLAGIARISM AND COPYRIGHT PROTECTION

Chenushkina Svetlana

Russian State Vocational Pedagogical University, Russia, Yekaterinburg

Аннотация . *В статье рассматривается техническая сторона защиты авторских прав. Описываются основные способы и методы защиты от плагиата.*