Эспергенов Асанбий Казмуханбетович

магистрант

БУ ВО ХМАО – Югры «Сургутский государственный университет»

г. Сургут, ХМАО – ЮГРА

РАЗРАБОТКА МЕТОДОВ И СРЕДСТВ ОБЕСПЕЧЕНИЯ СОХРАННОСТИ КОНТЕНТА В КОРПОРАТИВНЫХ СЕТЯХ

Аннотация*: в данной статье рассматриваются методы сохранности контента в пределах корпоративных сетей. Автором также указываются рекомендуемые средства для осуществления обеспечения сохранности контента. Подводя итоги, автор утверждает, что для сохранности информации нужно понимать, насколько важна хранимая информация и соответственно защищать её.*

Ключевые слова*: проектирование программного средства, разработка функционально-организационной схемы, перечень функциональных задач, контур программного средства.*

На современном этапе развития нашего общества информация становится одним из наиболее ценных и востребованных ресурсов, на сохранение и защиту которых выделяется все больше времени и средств. В связи с чем защита и сохранение информации является одним из важных процессов любой организации.

Корпоративная компьютерная сеть – является неотъемлемой частью системы управления и предназначена для решения научно-образовательных задач и задач управления на базе современных информационных технологий, обеспечивающих, в частности, ускорение принятия решений на основе:

– оперативного обмена данными между подразделениями;

– использование общих информационных ресурсов, размещенных в сети;

– доступа через единую компьютерную сеть к данным других интрасетей и глобальных сетей;

– использования электронной почты;

– организации централизованного хранилища данных с различным уровнем доступа к информации.

Специфика защиты информации в образовательной системе заключается в том, что образовательное учреждение – публичное заведение с непостоянной аудиторией, а также место повышенной активности «начинающих кибер-преступников». Основную группу потенциальных нарушителей здесь составляют студенты.

Предметом исследования являются методы обеспечения сохранности контента с помощью современных средств вычислительной техники.

Работы по обеспечению сохранности электронных документов можно разделить на три вида:

– обеспечение физической сохранности и целостности файлов с электронными документами;

– обеспечение условий для считывания информации в долговременной перспективе;

– обеспечение условий для воспроизведения электронных документов.

Целями обеспечения сохранности информации в локальной сети АНПОО «СИУЭП» являются:

– предотвращение угроз безопасности информации;

– защита законных интересов организации от противоправных посягательств на информацию в ЛВС;

– недопущение хищения информационных, финансовых и материально-технических ресурсов, уничтожения имущества и ценностей, разглашения, утраты, утечки, искажения и уничтожения служебной информации, нарушения работы технических средств, обеспечивающих производственную деятельность.

Для реализации поставленных целей, т.е. для модернизации системы обеспечения сохранности и безопасности информации необходимо выполнение следующих задач:

– разработка комплекса мероприятий по модернизации системы обеспечения безопасности информации в ЛВС.

– Рассмотрение организационных, программных и технических мероприятий (схема 1.).

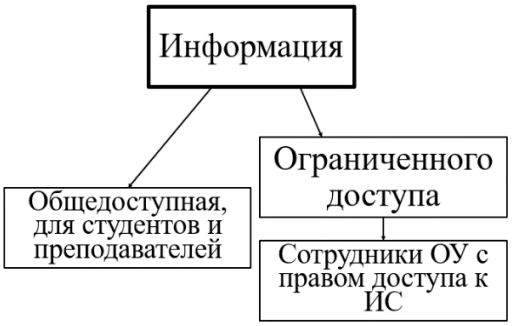

Схема 1.

Требования к системе:

– система должна обеспечивать сохранение целостности, доступности и конфиденциальности хранимой и обрабатываемой информации;

– система не должна изменять топологии существующей сети;

– система должна быть экономически выгодной.

Система обеспечения сохранности контента независимо от сферы их применения, как правило, включают один и тот же набор компонентов: функциональные компоненты; компоненты системы обработки данных; организационные компоненты.

Состав функций, реализуемых в системе обеспечения сохранности контента, подразделяется на информационные и управляющие функции (схема 2).

Схема 2.

В свою очередь, различают: информационные функции централизованного контроля и функции вычислительных и логических операций.

Примерный перечень задач, которые должна решать система обеспечения сохранности контента на различных уровнях управления предприятием и для различных его служб, к настоящему времени можно считать функциональную модель предприятия (схема 3).

Функциональная модель

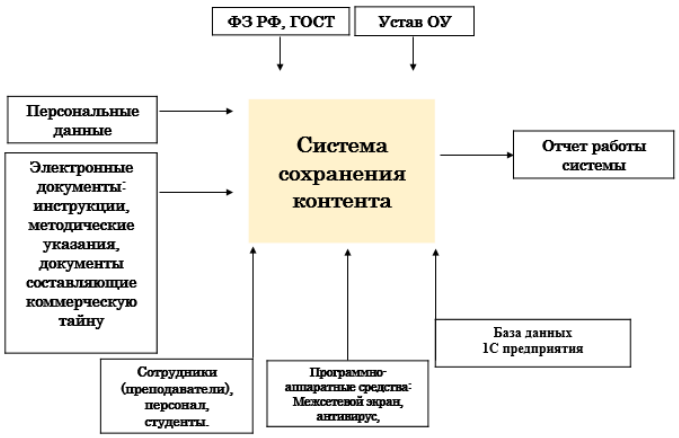

Схема 3

С учетом всех требований и принципов обеспечения сохранности информации по всем направлениям защиты в состав системы должны быть включены следующие средства:

– средства разграничения доступа к данным;

– средства криптографической защиты информации;

– средства регистрации доступа к компонентам информационной системы и контроля за использованием информации;

– средства реагирования на нарушения режима информационной безопасности.

На технические средства защиты и сохранения информации возлагается решение следующих функциональных задач (схема 4):

– идентификация и аутентификация пользователей при помощи имен или специальных аппаратных средств;

– регламентация и управление доступом пользователей в помещения, к физическим и логическим устройствам;

– защита от проникновения компьютерных вирусов и разрушительного воздействия вредоносных программ;

– регистрация всех действий пользователя в защищенном журнале, наличие нескольких уровней регистрации;

Защита данных системы защиты на файловом сервере от доступа пользователей, в чьи должностные обязанности не входит работа с информации, находящейся на нем.

Схема 4.

Какова бы ни была система защиты информации в конкретной организации, главное – помнить два основных правила.

Первое: комплексная защита информации – это, прежде всего, совокупность принятых в компании мер по защите, а не набор продуктов. Нельзя списывать со счетов и то, что в обеспечении информационной безопасности участвует каждый сотрудник компании.

Второе: основа любой системы защиты – это люди. От того, насколько грамотно персонал настроит эксплуатируемые системы, как он будет готов реагировать на инциденты в области безопасности, зависит защищенность предприятия в целом.

Что же касается технологий и конкретных средств защиты информации, то использование антивирусов, межсетевых экранов и механизмов разграничения

доступа обеспечивает лишь минимально необходимый уровень защищенности, а применение дополнительных механизмов защиты должно определяться экономической целесообразностью.

Список литературы

1. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации». [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 21.05.19).

2. СанПиН 2.2.2/2.4.1340–03 «Гигиенические требования к видеодисплейным терминалам, персональным электронно-вычислительным машинам и организации работы». [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/-document/901865498 (дата обращения: 21.05.19).

3. ГОСТ Р 54989–2012. [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/gost-r-54989-2012 (дата обращения: 21.05.19).

4. Федеральный закон от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи». [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения: 21.05.19).

5. [Электронный ресурс]. – Режим доступа: https://fstec.ru/ (дата обращения: 21.05.19).

6. [Электронный ресурс]. – Режим доступа: https://www.comss.ru/ (дата обращения: 21.05.19).

7. [Электронный ресурс]. – Режим доступа: https://sbis.ru/about/license (дата обращения: 21.05.19).

8. [Электронный ресурс]. – Режим доступа: https://www.esetnod32.ru/ (дата обращения: 21.05.19).

9. [Электронный ресурс]. – Режим доступа: https://www.dallaslock.ru/ (дата обращения: 21.05.19).