IV. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056:378

© Данилов А.Н., Шабуров А.С.
Danilov A., Shaburov A.

ОСНОВНЫЕ НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОТКРЫТЫХ ОБРАЗОВАТЕЛЬНЫХ СИСТЕМ

THE MAJOR DIRECTIONS TO ENSURE THE INFORMATION SECURITY OF THE OPEN EDUCA-TIONAL SYSTEM

Аннотация. *В статье предлагается подход к обеспечению информационной безопасности образовательной системы открытого типа, проводится анализ основных проблем защиты информации, связанных с модернизацией современных систем образования. Приводится модель обеспечения информационной безопасности открытой образовательной системы с учетом решения основных традиционных задач по защите информации.*

Annotation. *The article deals with the approach to ensure open educational system information security. The authors analyzed major information protection issues associated with modern educational system enhancement, and presented the open educational system information security model including a solution to main conservative objectives to protect information.*

Ключевые слова. *Информационная безопасность, образовательная система, информационная среда, управление системами образования, информационная технология, угроза информационной безопасности.*

Key words. *Information security, educational system, information space, education management, information technology, information security threat.*

Модернизация российского высшего образования предполагает принципиальное обновление его содержания, нацелена на новые образовательные результаты, прежде всего, на подготовку специалистов нового поколения. Это предусматривает существенное изменение параметров всей образовательной системы.

В качестве основных принципов модернизации системы образования должны использоватьсяе: повышение качества образования, его доступности и эффективности. Следовательно, главными направлениями модернизации системы управления образованием является необходимость управления качеством, доступностью образовательных ресурсов и эффективностью их использования [1].

Одним из главных условий достижения планируемых результатов является функционирование вузов в условиях открытости образовательных систем и наличие соответствующей современным требованиям образовательной среды, в которой этот результат, выраженный в виде сформированных компетенций выпускников вузов, будет достигнут.

Совершенствование системы управления образованием и переход на образовательные системы открытого типа предполагает как возможность выхода в глобальное информационное пространство со стороны се-

Данилов Александр Николаевич – кандидат технических наук, профессор, Пермский национальный исследовательский политехнический университет, тел. (342)219-85-71;
Шабуров Андрей Сергеевич – кандидат технических наук, доцент, Пермский национальный исследовательский политехнический университет, тел. (342)239-18-17.

Danilov Aleksandr –PhD, professor, the Perm national research polytechnic university, tel. (342)219-85-71;
Shaburov Andrey – PhD, associate professor, the Perm national research polytechnic university, tel. (342)239-18-17.

тевой подсистемы вуза в направлении внешних информационных ресурсов, так и возможность доступа в образовательную среду вуза со стороны внешних потребителей информации.

Образовательная система открытого типа динамична, имеет широкие контакты с внешним миром, ей характерна высокая степень интеграции на основе современных информационных технологий. При этом открытость образовательной среды, в свою очередь, создает ряд проблем, одной из которых является проблема обеспечения информационной безопасности.

Необходимость совершенствования процессов управления в вузе, и связанная с ней возрастающая актуальность угроз информационной безопасности, требует поиска новых концептуальных подходов для управления образовательными системами и, как следствие, решения задач по защите информационной образовательной среды. К таким задачам, прежде всего, относятся:

• обеспечение доступности (открытости) электронных образовательных ресурсов и индивидуальных авторских образовательных программ;

• обеспечение бесперебойного функционирования административной подсистемы и системы делопроизводства;

• защита информационных систем персональных данных (ИС ПДн) работников и учащихся вузов;

• обеспечение конфиденциальности результатов научных исследований и защита интеллектуальной собственности в процессе научно-исследовательской работы преподавателей и студентов.

Кроме того, процесс глобальной информационной интеграции, коммерциализация системы образования и повышение доступности разнообразных образовательных ресурсов порождает проблему конкуренции между образовательными учреждениями, как на международном, так и на внутригосударственном уровне. Это выражается не столько в экспорте образования, сколько в борьбе стран за высококвалифицированные кадры, а учебных заведений, - за наличие обучаемых и их качественный состав.

В данных условиях приоритетными задачами управления информационной безопасностью становится следующие:

• обеспечение максимальной степени доступности (открытости) образовательной системы для санкционированного пользователя;

• снижение степени открытости, вплоть до полной изоляции информационной системы, с целью оперативного реагирования на возникающие угрозы информационной безопасности, блокирование информационных атак, обеспечение конфиденциальности и целостности информационных ресурсов.

Анализ актуальных угроз информационной безопасности позволяет сформировать требования к защите информации для любой образовательной системы, которые могут быть определены на основе следующих источников:

1. Оценки рисков, с учетом общей деловой стратегии и целей организации, уязвимостей по отношению к случаю и вероятности его возникновения, а также его возможного негативного влияния.

2. Требования законов, устава вуза, других обязательных требований и требований договорных отношений, которые вуз, его партнеры, подрядчики и поставщики услуг должны выполнить, а также с учетом их взаимодействия в социально-культурной среде.

3. Конкретный набор принципов, целей и деловых требований к обработке информации, которые выработаны образовательным учреждением для поддержки выполнения своих задач.

Определение требований к защите информации, в свою очередь, позволит реализовать необходимый перечень методов и средств защиты, наиболее эффективные технологии управления информационной безопасностью и информационно-аналитической поддержки данного процесса.

Решение задач по защите информации целесообразно выполнять комплексно, на основе принципов системного подхода, применяя полный арсенал типовых и оригинальных методов и средств защиты информации.

Применение методов и средств защиты информации необходимо осуществлять на основе действующих государственных и отраслевых стандартов по информационной безопасности, с учетом внедряемых в настоящее время международных рекомендаций [2].

Защита информации должна работать как инструмент обеспечения конфиденциальности, целостности информации для того, чтобы избежать, или снизить соответствующие риски злоумышленного нанесения ущерба электронному контенту образовательной среды, в то же время, обеспечивая необходимый уровень доступности информации.

В целях повышения эффективности процесса управления образовательной системой вуза, управлением информационной безопасностью предполагается создание и развитие системы распределенных ситуационных центров, работающих по единому регламенту взаимодействия и осуществляющих необходимую

информационно-аналитическую поддержку.

На рисунке представлена структурная модель обеспечения информационной безопасности открытой образовательной системы вуза. Данная модель предусматривает решение основных задач, связанных с безопасностью:

• открытых электронных образовательных ресурсов;

• системы электронного документооборота (СЭД) – основы административной подсистемы вуза;

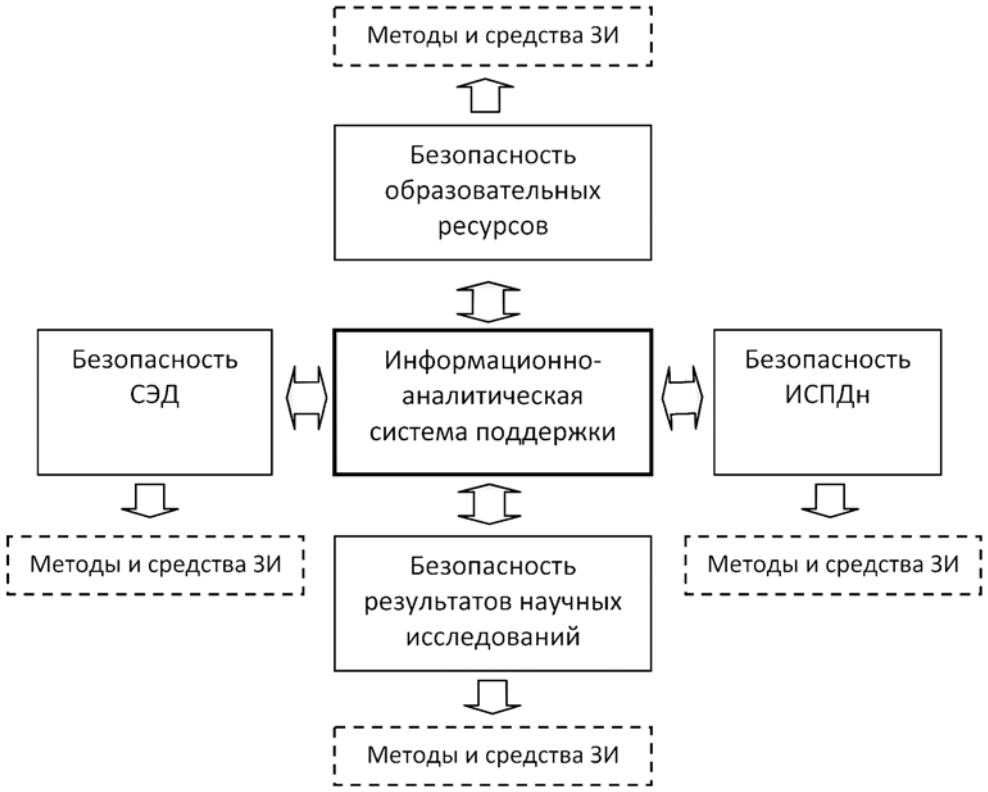
• информационных систем персональных данных (ИС ПДн) работников и учащихся вузов;

• научных исследований и результатов интеллектуальной деятельности.

Комплексность решения задач защиты информации и скоординированное применение методов и средств защиты информации обеспечивается подсистемой единой информационно-аналитической поддержки, что способствует повышению эффективности применения отдельных компонентов защиты.

Фактор информационных воздействий на социальную среду вуза посредством распространения вредоносной информации в данном случае моделью не предусматривается, так как в меньшей степени связан с технической защитой информации, обусловлен гуманитарными и психологическими аспектами, что требует дополнительных научных исследований.

Учитывая специфику деятельности в области предоставления образовательных услуг, в условиях внедрения дистанционных образовательных технологий, решение проблемы открытости и защищенности *образовательных ресурсов* становится первоочередной и наиболее ответственной задачей. В данном случае традиционно, предполагается оперативное управление доступом с помощью выбранных методов и средств защиты информации с целью повышения или уменьшения степени открытости образовательных ресурсов, в зависимости от категории лиц, доступ осуществляющих. При этом обеспечение конфиденциальности, целостности и доступности самих ресурсов непосредственно влияет на качество всего образовательного процесса.



Модель обеспечения информационной безопасности открытой образовательной системы

Взаимосвязь государственных и частных сетей и совместное использование информационных ресурсов увеличивает трудность достижения поставленных целей защиты и управления доступом. Курс на распределенную обработку данных также ослабляет результативность централизованного, специализированного управления. В данном случае существенное значение для защиты информации приобретает перечень пользователей информационных систем.

Информационное взаимодействие открытых об-

разовательных систем, как правило, предполагает участие следующих участников информационного обмена – пользователей информационных ресурсов:

• учащихся учебных заведений;

• профессорско-преподавательского состава учебных заведений;

• административно-управленческого аппарата учебных заведений;

• работодателей, заинтересованных в подготовке учащихся.

Кроме того, в информационном обмене предполагается участие государственных и частных структур, обеспечивающих образовательные системы, родственников учащихся, иных заинтересованных лиц. Вместе с тем предполагается вероятность воздействия на информационные ресурсы различных категорий злоумышленников. Средства защиты информации от несанкционированного доступа со стороны злоумышленников должны обеспечивать [3]:

1) контроль доступа к компьютерам, каталогам, файлам, логическим дискам в соответствии с условиями разграничения доступа;

2) автоматизированное формирование соответствующих видов реакции на обнаруживаемые попытки нарушения разграничения прав доступа;

3) протоколирование (регистрацию) доступа к информационным ресурсам в соответствии с условиями разграничения доступа и настройками, осуществляемыми в рамках администрирования системы. При этом должно настраиваться протоколирование нарушений определённого вида и срок, за который осуществляется ведение протокола;

4) блокирование доступа при подозрительных попытках использования информационных ресурсов;

5) защиту от несанкционированной модификации программного обеспечения, включая защиту от внедрения вредоносных кодов в программные продукты;

6) защиту информации от случайных разрушений;

7) защиту ввода и вывода информации на отчуждаемый физический носитель и установления соответствия (сличения) пользователя с устройством;

8) защиту от утечки информации по побочным каналам технических средств, предназначенных для обработки и хранения конфиденциальной информации.

При этом обеспечение оперативности доступа к образовательным ресурсам является не менее важной задачей для всей системы защиты информации (СЗИ) и ее информационно-аналитической поддержки.

На сегодняшний день критически важным, с точки зрения обеспечения информационной безопасности ресурсов образовательных систем, могут считаться *результаты научных исследований*, достижения области науки и техники, суть которых должна обрабатываться в режиме коммерческой тайны.

Современная государственная политика Российской Федерации в области модернизации системы образования и повышения ее эффективности направлена на внедрение наукоемких технологий, инновационного развития народного хозяйства, разнообразные формы международного сотрудничества.

Создание системы национальных исследовательских университетов предполагает открытие совместно с предприятиями научных лабораторий, интеграцию информационной образовательной среды в сферу промышленного производства и бизнеса. Подобные процессы, безусловно, повышают актуальность создания единой системы защиты как с точки зрения конфиденциальности и целостности плодов научных исследований и изобретений, так и с точки зрения сохранения авторского права на результаты интеллектуальной деятельности. Особенно это характерно для среды наукоемких и инновационных технологий, наиболее подверженным угрозам информационной безопасности в условиях конкурентной борьбы и промышленного шпионажа.

Наиболее важными объектами обеспечения информационной безопасности Российской Федерации в области науки и техники являются [4]:

• результаты фундаментальных, поисковых и прикладных научных исследований, потенциально важные для научно - технического, технологического и социально - экономического развития страны, включая сведения, утрата которых может нанести ущерб национальным интересам и престижу Российской Федерации;

• открытия, незапатентованные технологии, промышленные образцы, полезные модели и экспериментальное оборудование;

• научно - технические кадры и система их подготовки;

• системы управления сложными исследовательскими комплексами.

Процесс защиты информации подобного характера может осуществляться на основе традиционных принципов и технологий информационной безопасности для сведений, составляющих коммерческую тайну.

Эффективность управления образовательными системами во многом зависит от решения задач оперативного и качественного формирования электронных

документов, контроля их исполнения, а также продуманной организации их хранения, поиска и использования.

Потребность в эффективном управлении электронными документами привела к созданию систем электронного документооборота (СЭД), под которыми понимают организационно-технические системы, облегчающие процесс создания, управления доступом и распространения электронных документов в компьютерных сетях, а также обеспечивающие контроль над потоками документов в образовательном учреждении [5].

В последнее время развитие СЭД направлено в основном на совершенствование сервисных возможностей, так как базовые возможности в той или иной форме уже реализованы. Кроме того, можно отметить развитие СЭД в сторону управления различного вида контентом (мультимедиа), использование технологий автопроцессинга и разбора содержания документа.

Ряд существующих СЭД позволяет вести электронные архивы, наполнение которых происходит через системы потокового сканирования и ввода бумажных документов, автоматизированной обработки электронной почты, а также запросов и обращений, поступающих через ведомственные интернет-сайты. Используемые системы обеспечивают прохождение этих документов до структурного подразделения или подведомственной организации, учет и контроль своевременности их рассмотрения и исполнения.

Наличие электронного архива создает основу для совершенствования системы управления вузом, доступа и интеграции управляющей информации. С его помощью можно объединить все формы данных: документы, Web, изображения и аудиовизуальную информацию – в различных рабочих процессах и приложениях. Участники процесса получают возможность составлять, заполнять, просматривать, редактировать, визировать и публиковать документы в электронной форме с высокой степенью безопасности и с использованием Интернета или Интранета. Таким образом, СЭД позволяет:

• обеспечить высокую доступность и безопасность информации;

• поддерживать работу ключевых систем организаций;

• существенно сократить расходы на хранение и управление цифровой информацией;

• снизить убытки из-за потерь важных документов.

При всех преимуществах внедрение СЭД порождает новые риски, и пренебрежение защитой приводит к новым информационным угрозам.

В общем случае к задаче создания СЭД необходимо подходить с точки зрения традиционной защиты информационной системы, обеспечивая решение следующих задач:

• аутентификацию пользователей и разделение доступа;

• подтверждение авторства электронного документа;

• контроль целостности электронного документа;

• конфиденциальность электронного документа;

• обеспечение юридической значимости электронного документа.

Разработка СЗИ СЭД должна проводиться с учетом защиты от выявленных угроз и возможных информационных рисков, для которых определяются способы защиты, и на основе предложенного показателя оценки ее эффективности. При этом учитываются основные требования, которые предъявляются к созданию СЗИ, а именно:

• обеспечение контроля и регистрации попыток НСД, содержание средства для точного установления идентичности каждого пользователя и проведение протоколирования действий;

• обеспечение надежности защиты информации и контроль за функционированием системы защиты, т.е. использование средств и методов контроля работоспособности механизмов защиты.

Реализация перечисленных требований при создании СЗИ в СЭД будет качественно влиять на процесс функционирования административной подсистемы вуза и способствовать повышению уровня информационной безопасности образовательной среды в целом.

Обеспечение защиты информационных систем персональных данных (ИСПдн) является специфической и достаточно регламентированной деятельностью любой организации – оператора персональных данных и базируется на требованиях действующего законодательства Российской Федерации и нормативных документах ФСЭК России. Реализация данных требований должна осуществляться в рамках единой системы управления информационной безопасностью с учетом комплексного применения методов и средств защиты информации.

С учетом вышеизложенного можно определить следующие обязательные этапы работы по защите персональных данных в вузах:

• определение перечня персональных данных, необходимых для предоставления образовательных услуг;

• определение всех ситуаций, когда требуется обработка персональных данных;

• выделение процессов и ситуаций, связанных с

обработкой персональных данных;

• разработку перечня подразделений и работников, участвующих в обработке персональных данных в рамках своей служебной деятельности;

• определение круга информационных систем, предназначенных для обработки персональных данных;

• проведение категорирования персональных данных и классификации информационных систем;

• анализ угроз безопасности персональных данных при их обработке;

• разработку пакета организационно-распорядительных документов для обеспечения защиты персональных данных (положения, приказы, акты, инструкции и т. п.);

• проектирование и внедрение системы защиты ИСПДн.

Таким образом, определение требований защиты и выявление рисков позволяет выбрать и внедрить соответствующие средства управления информационной безопасностью с целью обеспечить снижение рисков до приемлемого уровня. Средства управления могут быть выбраны из этого стандарта или из других наборов средств управления, или же могут быть разработаны вновь с целью удовлетворить конкретные потребностей защиты информации. Выбор средств управления защитой зависит от организационных решений, основанных на критериях оценки угроз, вариантах обработки рисков и на общем подходе к управлению рисками, применяемом в образовательной системе. Кроме того, выбор механизмов безопасности должен подчиняться всем применимым национальным и международным законам и нормам. Комплексное применение методов и средств защиты и единая информационно-аналитическая поддержка обеспечит необходимые качественные характеристики и, в первую очередь – эффективность управления образовательными системами.

Литература

1. Новиков Д. А. Введение в теорию управления образовательными системами. – М.: Эгвес, 2009. – 156 с.

2. ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security management (Информационные технологии. Свод правил по управлению защитой информации).

3. ГОСТ Р 51241-98. Государственный стандарт Российской Федерации средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.

4. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 № Пр-1895).

5. Булдакова Т.И., Глазунов Б.В., Ляпина Н.С.. Оценка эффективности защиты систем электронного документооборота // Математическое обоснование и теоретические аспекты информационной безопасности /Доклады ТУСУР: № 1 (25), часть 2, 2012. - С. 52-56.

Материал поступил в редакцию 11. 12. 2012 г.