

Предложенная система и разработанная АИС позволяют автоматизировать процесс развития ППС в ВУЗе на этапе выбора индивидуальной траектории, а их внедрение в свою очередь позволит сократить временные и финансовые затраты на организацию повышения компетентности специалистов.

Библиографический список

1. Е.В. Ларина Механизм управления высшим учебным заведением на основе развития ключевой компетенции // Электронное научно-техническое издание «Наука и образование» №12, декабрь 2011 г.
2. О.М. Гергерт, О.Г. Берестнева, Я.С. Пеккер Автоматизированная информационная система оценки адаптации развивающихся систем // Информационные технологии в системах автоматизации.

С.У. Увайсов, И.В. Аютова
(Москва), (Сургут)

Информационные технологии защиты персональных данных в вузе

В вузах реализуются различные по срокам и уровню подготовки специалистов образовательные программы [1]. При этом вуз, как объект исследования, обладает рядом особенностей [2, 3, 4, 5] таких как публичность, непостоянство аудитории, широкое внедрение средств вычислительной техники, территориальная разобщенность отдельных объектов, использование современных информационных технологий, развитие различных форм дистанционного обучения. В силу своей специфики в вузе хранится и обрабатывается огромное количество информации, связанной с обеспечением учебного процесса, внеучебной деятельности, научных разработок, международного сотрудничества, служебная, коммерческая и иная конфиденциальная информация, в том числе персональные данные (ПДн) студентов, сотрудников, посетителей, абитуриентов, и других категорий субъектов ПДн.

ПДн это важная и ценная информация о человеке, и государство требует от операторов, обрабатывающих ПДн, выполнение требований законодательства. Вузы являются операторами ПДн, и соответственно, на них распространяется действие законодательства. Защита персональных данных является сложной, трудоемкой, затратной работой, ненадлежащее исполнение которой может обернуться значительными негативными последствиями для организации и граждан, чьи сведения обрабатываются.

Комплекс мероприятий по приведению информационных систем обработки персональных данных (ИСПДн) вуза требованиям законодательства включает в себя несколько этапов, ключевым этапом является предпроектное обследование ИСПДн. При проведении предпроектного обследования трудности у операторов вызывают построение моделей угроз и определение классов ИСПДн. Данные этапы предпроектного обследования существенно увеличивают финансовые издержки и временные затраты.

В настоящий момент существуют следующие информационные технологии, автоматизирующие процесс разработки моделей угроз:

1. Программный комплекс «WingDoc ПД» [6] (г. Екатеринбург, ООО «Компания информационных технологий»);

2. Программная система оценки и построения модели угроз безопасности ПДн «АИСТ-П» [7] (г. Томск, ТУСУР, Миронова В.Г.);

3. Программное обеспечение «Модели угроз медицинских информационных систем» (г. Томск, ТУСУР, Зыков В.Д.);

4. Программа оценки и построения модели воздействий на персональные данные вуза «ПЕРС».

1. Программный продукт «WingDoc ПД» предназначен для специалистов отделов, занимающихся защитой информации, сотрудников отделов информационных технологий, организаций, которые профессионально занимаются защитой информации.

Программный комплекс позволяет в полуавтоматическом режиме создать модель воздействий.

Программа имеет модульную архитектуру. В состав программы входят следующие модули для разработки моделей воздействий:

Модуль «Модель угроз ИСПДн».

Модуль выполняет автоматическое составление модели воздействий согласно нормативно-методическому документу ФСТЭК России «Методика определения актуальных угроз безопасности ПДн при их обработке в ИСПДн» [8].

Модуль «Модель угроз ИСПДн-К»

Модуль составляет модель воздействий и источника воздействий в соответствии с нормативно-методическим документом ФСБ России «Методические рекомендации по обеспечению с помощью криптосредств безопасности ПДн при их обработке в ИСПДн с использованием средств автоматизации» [9].

2. Программная система оценки и построения модели воздействий на информационные системы обработки ПДн «АИСТ-П» предназначена для автоматизации этапов классификации ИСПДн, определения

степени исходной защищенности ИСПДн и разработки модели воздействий (в соответствии с требованиями ФСТЭК России и ФСБ России [8,9,10]).

Разработка модели угроз производится с помощью экспертных оценок каждой из возможных угроз безопасности ПДн. В результате работы программы формируются документы:

- акт классификации ИСПДн;
- модель угроз ИСПДн.

3. Программное обеспечение «Модели угроз медицинских информационных систем» [11].

Пользователь, с использованием программного обеспечения проводит классификацию медицинской информационной системы (МИС). Классификация осуществляется в ходе опроса пользователя. В результате формируется акт классификации, модель воздействий и перечень рекомендуемых организационно-технических мероприятий.

Особенностью данного программного обеспечения – возможность его использования специалистами системы здравоохранения, не имеющими специальных знаний в области защиты информации. В данном программном обеспечении происходит объединение на этапе предпроектного обследования этапов классификации ИС и разработки модели воздействий за счет типизации.

Перечисленные инструментальные средства не учитывают специфику вуза, и при проведении предпроектного обследования с использованием программного комплекса «WingDocПД» и системы оценки и построения модели воздействий на ПДн «АИСТ-П» необходимо привлечения узко квалифицированных специалистов сторонних организаций, что приводит к увеличению финансовых затрат вуза.

4. Программа оценки и построения модели воздействий на персональные данные вуза «ПЕРС».

Программный комплекс включает в себя три модуля:

- Классификация ИСПДн;
- Определение степени исходной защищенности ИСПДн;
- Построение модели внешних воздействий вуза.

Разработанный программный комплекс в отличие от аналогов учитывает специфику вуза. Сравнение программного обеспечения по ключевым параметрам представлено в таблице 1.

Разработанный комплекс «ПЕРС» обладает следующими достоинствами, во-первых, учитывает специфику вуза, во-вторых, за счет типизации информационных систем обработки ПДн, удалось существенно сократить количество вопросов пользователя, и, в-третьих, использо-

вание данного комплекса не требует привлечения сторонних специалистов.

Оценка эффективности разработанного программно-методического комплекса «ПЕРС» проведена для ИСПДн ГОУ ВПО «Сургутский государственный университет ХМАО - Югры». Предложения на выполнение комплекса мероприятий по приведению информационных систем обработки ПДн ГОУ ВПО «Сургутский государственный университет ХМАО - Югры» были переданы в соответствующие организации. Согласно коммерческим предложениям от компаний, которые согласились выполнить данный комплекс мероприятий, построена таблица 2.

Таблица 1

Сравнение программного обеспечения

Название	Методики разработки модели угроз	Необходимые сведения	Количество вопросов пользователю	Предполагаемые пользователи	Типы ИСПДн
Программный комплекс «WingDoc ПД» (Екатеринбург, ООО «Компания информационных технологий»)	ФСТЭК России	Эксплуатационные характеристики, сведения об условиях функционирования ИСПДн	80-95	Специалисты по защите информации	Все
	ФСБ России	Сведения об условиях функционирования ИСПДн	25-30	Специалисты по защите информации	Все
Программная система оценки и построения модели угроз безопасности ПДн «АИСТ-П» (Томск, ТУСУР, Миронова В.Г.)	ФСТЭК России, ФСБ России	Эксплуатационные характеристики ИСПДн, экспертные оценки вероятности и опасности угроз	53-71	Специалисты по защите информации	Все

Программное обеспечение «Модели угроз медицинских информационных систем» (г. Томск, ТУСУР, Зыков В.Д.).	ФСТЭК России, Минздрав-соцразвития России, ФСБ России	Эксплуатационные характеристики МИС	5-10	Специалисты учреждения системы здравоохранения	МИС
Программа оценки и построения модели воздействий на персональные данные вуза «ПЕРС»	ФСТЭК России, Министерство образования	Эксплуатационные характеристики, сведения об условиях функционирования ИСПДн	14-15	Специалисты вуза	ИСПДн вуза

Таблица 2

**Стоимость работ по приведению ИСПДн вуза
к требованиям законодательства**

	ЗАО «ЛЕТА»	ЗАО «НТЦ МИК-ИНФОРМ»	ООО «Поинт-лэйн»
Стоимость проекта по обеспечению защиты ПДн, руб.	893 571	514 000	1 579 040
Сроки выполнения проекта, нормированные рабочие дни	46	106	214
Стоимость проведения классификации ИСПДн и построения модели воздействий, руб.	Стоимость не включает в себя построение модели воздействий	160 000-260 000	409 120
Временные затраты на проведение классификации ИСПДн и построения модели воздействий, нормированные рабочие дни	Стоимость не включает в себя построение модели воздействий	20	29

На рис. 1-2 представлены графики, демонстрирующие эффективность использования разработанного программно-методического комплекса. Из графиков видно, что при использовании разработанного комплекса происходит сокращение временных и финансовых затрат.

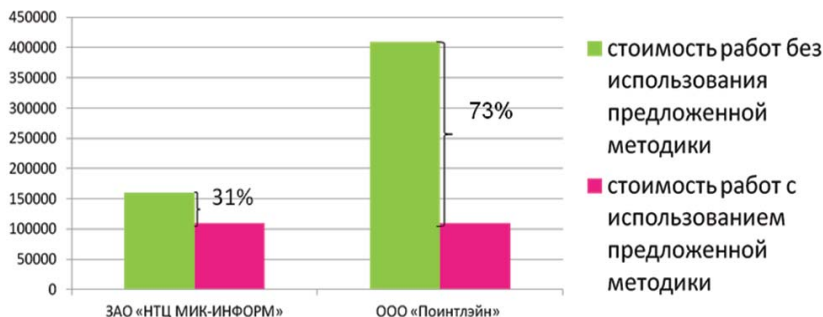


Рис. 1. Снижение финансовых затрат на этапе классификации ИСПДн и построения модели воздействий

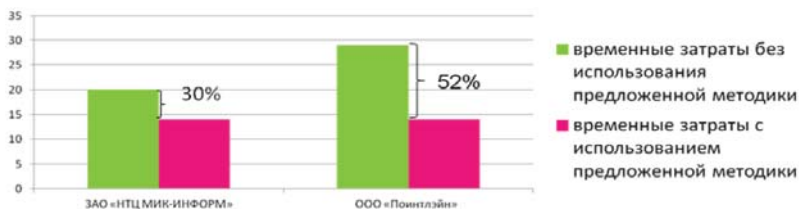


Рис. 2. Снижение временных затрат на этапе классификации ИСПДн и построения модели воздействий

Как видно из графиков при применении разработанного программно-методического комплекса происходит снижение финансовых затрат на 31 % и временных на 30%, при условии если воспользоваться услугами ЗАО «НТЦ МИК-ИНФОРМ». Если воспользоваться услугами ООО «Поинтлэйн» экономия будет составлять 73% и 52% соответственно.

Предоставление вузом образовательных услуг сопровождается обработкой ПДн студентов, преподавателей, сотрудников, абитуриентов и других субъектов ПДн. Вуз как оператор, обрабатывающий ПДн, обязан выполнять требования законодательства. Для сокращения издержек связанных с привлечением сторонних специалистов по защите информации на этапе предпроектного обследования в работе разработан программно-методический комплекс «ПЕРС». Использование данного комплекса позволяет существенно повысить эффективность управления

процессом обработки ПДн в вузе, снижая финансовые и временные затраты на этапе предпроектного обследования.

Библиографический список

1. Устав СурГУ [Электронный ресурс]. - Режим доступа: <http://www.surgu.ru/index.php?view=s&sid=64>.
2. Васильев, В.И. Построение нечетких когнитивных карт для анализа и управления информационными рисками вуза / В.И. Васильев, И.А. Савина, И.И. Шарипова // Вестник Уфимского государственного авиационного технического университета. Серия: Управление, вычислительная техника и информатика. - 2008. - Т. 10, №2. - С. 199–209.
3. Гузаиров, М.Б Системный анализ информационных рисков вуза с применением нечетких когнитивных карт / М.Б. Гузаиров, В.И. Васильев, Р.Т. Кудрявцева // Инфокоммуникационные технологии. - 2007. - №4. - С. 96-101.
4. Костюкова, Т.П. Образовательное учреждение как объект управления в условиях риска / Т.П. Костюкова, И.А. Лысенко // Вестник УГАТУ. - 2011. - №5. - С. 208-205.
5. Проталинский, О.М. Информационная безопасность вуза / О.М. Проталинский, И.М. Ажмухамедова // Вестник АГТУ. - 2009. - №1. - С. 18-23.
6. Программный комплекс WingDoc ПД модель угроз ИСПДн [Электронный ресурс]. - Режим доступа: http://www.wingdoc.ru/products/wingdoc_pd/.
7. Шелупанов, А.А. Автоматизированная система предпроектного обследования информационной системы персональных данных «АИСТ-П» / А.А. Шелупанов, В.Г. Миронова, С.С. Ерохин, А.А. Мицель // Доклады Томского государственного университета систем управления и радиоэлектроники. - 2010. - №1(21). - С. 14-22.
8. Нормативно-методический документ ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 14 февраля 2008 года.
9. Нормативно-методический документ ФСБ России «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» от 21 февраля 2008 года.
10. Нормативно-методический документ ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 14 февраля 2008 года.
11. Зыков, В.Д. Модели и средства обеспечения управления информационной безопасностью медицинских информационных систем: дис. ... кандидата технических наук: 05.13.19 / Зыков Владимир Дмитриевич. - Томск, 2010. - 150 с.