УДК 004.056

ЗАЩИТА ИНФОРМАЦИОННЫХ РЕССУРСОВ И ПРОЦЕССОВ В ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЯХ

К.В. Масалова, Е.В. Шарлаев

В статье рассматриваются проблемы защиты информационных систем персональных данных в высших учебных заведениях и построения эффективной системы защиты информационных систем персональных данных, а так же приводится алгоритм определения уровня защищенности информационных систем персональных данных в зависимости от реальных условий её функционирования. На примере реального объекта рассматривается один из путей решения данной проблемы – обращение к специалистам по защите информации, работающих на коммерческой основе.

Ключевые слова: информационные системы персональных данных, защита персональных данных, персональные данные, уровень защищенности ИСПДн

Актуальность

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 информация, относящаяся к физическому лицу, и государство требует от операторов, обрабатывающих ПДн, выполнение требований законодательства. ВУЗы являются операторами ПДн, и соответственно, на них распространяется действие закона о 152-ФЗ «О персональных данных».

Практика показывает, что разработать эффективную систему защиты информационных систем можно только в соответствии с действующими требованиями руководящих документов и рекомендаций. В них отражены требования, предъявляемые к построению системы защиты, выбору средств и методов защиты: программно-аппаратных, инженерно-технических, организационно-правовых.

Самостоятельно ВУЗ не всегда способен справиться с задачей построения эффективной системы защиты информации, поэтому прибегают к услугам коммерческих организаций, оказывающих услуги в области защиты информации. Это увеличивает расходы на защиту ПДн, но гарантирует более качественную работу и отлаженную систему защиты информации с полным пакетом документации.

Основными проблемами, с которыми сталкиваются при организации защиты ПДн в ВУЗе, являются:

- территориальная рассредоточенность ресурсов информационных систем;
- большое количество серверов, к которым привязаны ИСПДн, порой с разными уровнями защищенности;
- выход многих ИСПДн в глобальные сети и сети общего пользования.

Поэтому самым разумным подходом будет являться рассмотрение каждой ИСПДн отдельно, а уже затем рассматривать их в совокупности.

В соответствии с Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», требования по защите персональных данных в ИСПДн зависят от уровня защищенности ИСПДн.

Все ИСПДн по категориям обрабатываемых данных делятся на:

- обрабатывающие специальные категории персональных данных (касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни) (ИСПДн-С);

- обрабатывающие биометрические категории персональных данных (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта) (ИСПДн-Б);

- обрабатывающие иные персональных данных (ИСПДн-И).

- обрабатывающие общедоступные персональные данные (данные субъектов персональных данных, полученные только из общедоступных источников) (ИСПДн-О).

Отдельно выделены информационные системы, обрабатывающие персональные данные только сотрудников оператора.

В постановлении приведены три типа актуальных угроз.

- 1 тип. Угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении (операционная система)

- 2 тип. Угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении (программы обработки ПДн)

- 3 тип. Угрозы, не связанные с наличием недокументированных (недекларированных) возможностей

При этом в документе не дается указаний на способы выявления недекларированных возможностей программного обеспечения.

Если программное обеспечение лицензионное, выпускается серийно и имеет широкое распространение, то с большой долей вероятности можно сказать, что недекларированные возможности в нем отсутствуют. В противном случае есть высокая вероятность наличия недокументированных функций, способных нанести вред.

В таблице 1 наглядно представлен процесс определения уровня защищенности для ИСПДн

Таблица 1. - Определение уровня защищенности ИСПДн в соответствии с нормами действующего законодательства

Тип ИСПДн	Сотрудники оператора	Количество субъектов	Тип актуальных угроз		
			1	2	3
ИСПДн-С	Нет	> 100 000	УЗ1	УЗ1	УЗ2
	Нет	< 100 000	УЗ1	УЗ2	УЗ3
	Да				
ИСПДн-Б			УЗ1	УЗ2	УЗ3
ИСПДн-И	Нет	> 100 000	УЗ1	УЗ2	УЗ3
	Нет	< 100 000	УЗ-2	УЗ3	УЗ4
	Да				
ИСПДн-О	Нет	> 100 000	УЗ2	УЗ2	УЗ4
	Нет	< 100 000	УЗ2	УЗ3	
	Да				

Рассмотрим реальную ситуацию. В ВУЗе имеется структура сети, представленная на рисунке 1.

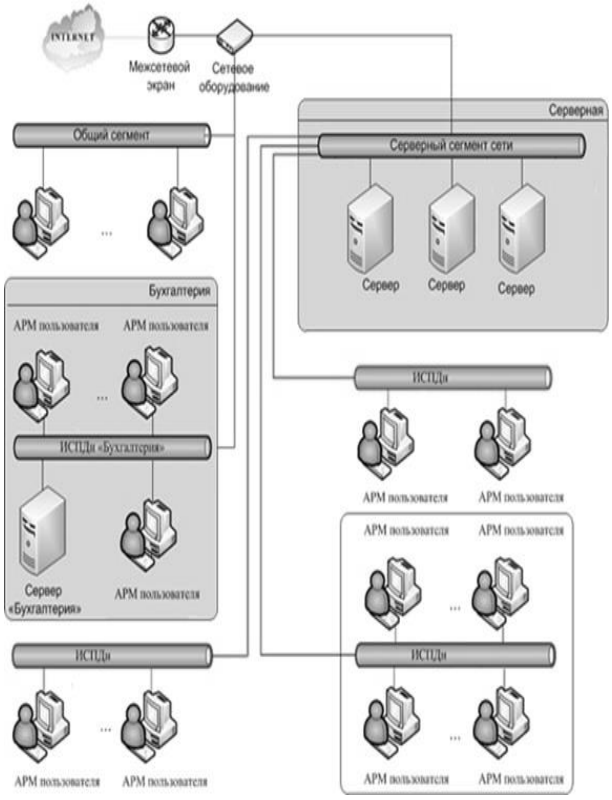

Рисунок 1 - Структурная схема сети ВУЗа

АРМ пользователей одной ИСПДн находятся в разных зданиях, у пользователей, как правило, различные права доступа к обрабатываемой информации в зависимости от цели обработки. Подключение к сети Интернет осуществляется по выделенной линии. Межсетевое экранирование от сети Интернет осуществляется не сертифицированными межсетевыми экранами. В зданиях ВУЗа введен пропускной режим, что не допускает несанкционированный доступ в помещения университета. В помещениях установлены системы пожарно-охранной сигнализации, двери помещений в нерабочее время закрываются на замок.

Типичная ситуация для ВУЗа это обработка специальных ПДн субъектов которые могут являться или не являться сотрудниками оператора в количестве до 100 000, актуальные угрозы третьего типа (для АС). Модель угроз строится на основе «Базовой модели угроз безопасности персональных данных при их обработке в информационных си-

стемах персональных данных» разработанной ФСТЭК России в 2008 году. То есть, большая часть ИСПДн будет отнесена к 3 уровню защищенности, однако встречаются ИСПДн с другим уровнем защищенности.

Разногласия между заказчиком (ВУЗом) и исполнителем возникают в основном в части устанавливаемого ПО и оборудования - денежных средств не всегда хватает для проведения полного объема мероприятий. Приказ ФСТЭК России от 18.02.2013 № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" предусматривает наличие компенсирующих мер при невозможности выполнения обязательных, но и этого не всегда достаточно и прибегают к понижению уровня защищённости. Если в ИСПДн обрабатывается биометрическая информация вместе с иными ПДн, то ищут пути убрать её из процесса обработки. Пример – фото сотрудника на пропуск хранится в ИСПДн, для неё характерны угрозы 3 типа, следовательно, ИСПДн можно отнести к 3 УЗ, но если фото на пропуск вклеивает сам сотрудник, а из ИСПДн фото удаляется, то уровень защищенности может понизиться до 4. Это значит, что большинство требований перестают быть обязательными для выполнения, можно сократить расходы на техническую и программную составляющую системы защиты и обойтись только организационными мерами защиты.

В нашем примере все ИСПДн имеют 3 УЗ, соответственно для выполнения большинства требований на АРМ и серверах оказалось достаточно установить антивирус, СЗИ НСД с токеном и персональный межсетевой экран соответствующих классов и сертифицированных ФСБ и ФСТЭК России. При выборе данных средств защиты руководствовались как эффективностью, так и экономической целесообразностью. Все СЗИ имеют централизованное управление и управляются администратором безопасности или штатным специалистом по защите информации.

На данный момент в данном учебном заведении уже установлена и настроена данная система защиты персональных данных. Все СЗИ настроены в соответствии с матрицей доступа. Так же были разработаны инструкции для операторов ИСПДн и администраторов безопасности. Система успешно функционирует, сообщений об ошибках и сбоях не поступало.

ВУЗ, как оператор ПДн, успешно прошел проверку государственных регуляторов на предмет выполнения требований закона №152-ФЗ «О персональных данных».

Выводы

В силу ряда особенностей операторам ПДн сложно самостоятельно разработать, установить и настроить эффективную, отвечающую всем требованиям законодательства систему защиты, поэтому в нашем регионе они чаще всего прибегают к услугам коммерческих предприятий, занимающихся информационной безопасностью. Они предлагают ВУЗу индивидуальные проекты, которые согласовываются на всех этапах построения и, при наличии жестких рамок, не позволяющих реализовать ни один из предложенных проектов, ищут альтернативные пути защиты или ухода от защиты.

СПИСОК ЛИТЕРАТУРЫ

1. Российская Федерация. Государственная дума. О персональных данных: [Федеральный закон от 27 июля 2006 № 152-ФЗ] // Рос.газ - 2006. - 29 июля - С.6.
2. Российская Федерация. Правительство. Об утверждении требований к защите персональ-
ных данных при их обработке в информацио
нных системах персональных данных: [Постановление Правительства РФ от 01.11.2012 № 1119] // Рос.газ - 2012. - 7 ноя. - С.19.
3. Российская Федерация. Федеральная служба по техническому и экспортному контролю.
Об утверждении Состава и содержания орг
анизационных и технических мер по обеспе
чению безопасности персональных данных
при их обработке в информационных систе
мах персональных данных: [Приказ ФСТЭК России от 18.02.2013 № 21] // Рос.газ - 2013. - 22 мая - С.19.

*Студент **К.В Масалова**, fish.koi.carp@gmail.com; к.т.н., доцент **Е.В. Шарлаев** - Алтайский Государственный технический университет, кафедра вычислительных систем и информационной безопасности, (385-2)29-07-86.*