

- родного информационного обмена» от 12 мая 2004 года N 611//
Собрание законодательства РФ, 17.05.2004, № 20, Ст. 1938;
4. Тропинина Т. Л. Киберпреступность и кибертерроризм: поговорим о понятийном аппарате: Сборник научных трудов международной конференции «Информационные технологии и безопасность». Выпуск 3. – К.: Национальная академия наук Украины, 2003. – 178-179 с;
 5. Уголовный Кодекс Республики Казахстан от 16.07.1997 № 167-I (в ред. 07.03.2014) // «Ведомости Парламента», 1997 г., № 15, Ст. 211.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПДн В ВУЗе

К.В. Масалова, АлтГТУ, факультет информационных технологий, 5 к.

Научный руководитель – *Е.В. Шарлаев*, к.т.н., доцент.

В силу своей специфики в ВУЗе хранится и обрабатывается огромное количество информации, в том числе персональные данные (ПДн) различных категорий субъектов ПДн. ВУЗы являются операторами ПДн, и соответственно, на них распространяется действие закона о 152-ФЗ «О персональных данных» [1].

Выполнив анализ нормативно-правовой базы, а также практического опыта в области информационной безопасности становится очевидным, что разработать эффективную систему защиты информационных систем можно только в соответствии с требованиями руководящих документов и рекомендаций.

ВУЗы, как правило, обращаются к коммерческим организациям, оказывающим услуги в области защиты информации. Это увеличивает расходы на защиту ПДн, но гарантирует наличие отлаженной системы 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 инфо-телекоммуникационные 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», требования по защите персональных данных в ИСПДн зависят от уровня защищенности ИСПДн [2].

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 системах 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.

В реальном ВУЗе, который брался за основу разработки, ИСПДн имеют 3 УЗ, соответственно для выполнения большинства требований на АРМ и серверах оказалось достаточно установить антивирусное средство, 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.

На данный момент в учебном заведении уже установлена и настроена данная система защиты персональных данных. Все СЗИ настроены в соответствии с матрицей доступа. ВУЗ, как оператор ПДн, успешно прошел проверку государственных регуляторов на предмет выполнения требований закона №152-ФЗ «О персональных данных».

В силу ряда особенностей операторам ПДн сложно самостоятельно разработать, установить и настроить эффективную, отвечающую всем требованиям законодательства систему защиты, поэтому 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 позво-

ляющих реализовать ни один из предложенных проектов, ищут альтернативные пути защиты или ухода от защиты.

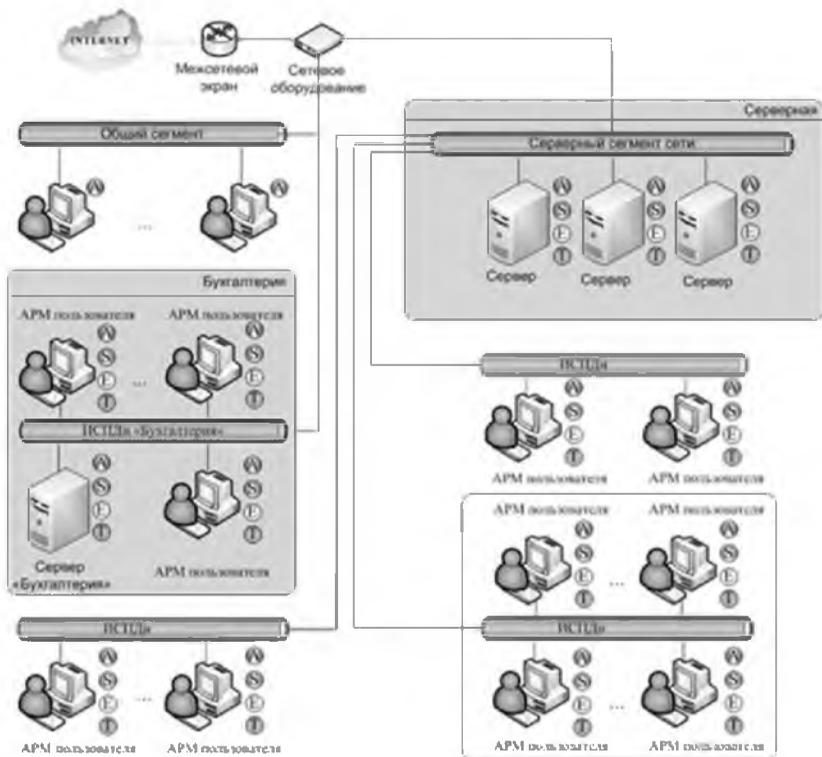


Рис.1 Проект системы защиты персональных данных.

Список литературы

1. О персональных данных: Федеральный закон от 27 июля 2006 № 152-ФЗ (ред. от 23.07.2013 N 205-ФЗ): [Электронный ресурс] – электронные данные. – Программа информационной поддержки российской науки и образования // справочные правовые системы Консультант Плюс: Высшая школа. – 2013. – Режим доступа: <http://www.consultant.ru>.
2. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: Постановление Правительства РФ от 01.11.2012 № 1119: [Электронный ресурс] – электронные данные. – Програм-

- ма информационной поддержки российской науки и образования // справочные правовые системы Консультант Плюс: Высшая школа. – 2013. – Режим доступа: <http://www.consultant.ru>.
3. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: Приказ ФСТЭК России от 18.02.2013 № 21: [Электронный ресурс] – электронные данные. – Программа информационной поддержки российской науки и образования // справочные правовые системы Консультант Плюс: Высшая школа. – 2013. – Режим доступа: <http://www.consultant.ru>.

ПРОБЛЕМЫ ОПТИМАЛЬНОСТИ КОНСТРУКЦИИ СТАТЬИ 183 УК РФ

И.С. Паришков, АлтГУ, юридический факультет, 2 к.
Научный руководитель – *В.А. Мазуров*, к.ю.н., доцент.

Актуальность темы выступления заключается в наличии проблем теоретического и практического характера, требующих разрешения.

Так, преступления, предусмотренные статьей 183 УК РФ носят высоко латентный характер, возбуждению уголовных дел во многом оказывает препятствие конструкция указанной статьи.

Ряд ученых правоведов (в частности, Паршин С.М. [1], Мазуров В.А. [2]) полагают, что было бы целесообразным выделить в самостоятельную статью УК РФ ответственность за налоговую тайну, так как по сути это служебная тайна, которая имеет некоторые существенные отличия от коммерческой и банковской тайны.

На основании ФЗ «О коммерческой тайне» [3] под коммерческой тайной понимается режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду; информация, составляющая коммерческую тайну (секрет производства), – сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах ин-