Тип работы: Отчет по практике

Предмет: Государственное и муниципальное управление

СОДЕРЖАНИЕ

СОДЕРЖАНИЕ 2
1. Общая характеристика места проведения практики 3
1.1 Организационная структура 3
1.2 Анализ основных нормативных документов 7
1.3 Анализ основных направлений деятельности 8
2. Экспериментальный раздел 13
3. Конструктивно-практический раздел 21
Список использованной литературы 24

В ходе активных дискуссий с гражданским обществом и профессиональными сообществами в 2013-2014 годах, Комитет принял важные законы, направленные на поддержание стабильности качества и устойчивости функционирования отечественного сегмента международной коммуникационной сети Интернет. Это Федеральный закон от 31 декабря 2014 года № 531-ФЗ «О внесении изменений в статьи 13 и 14 Федерального закона «Об информации, информационных технологиях и о защите информации» и Кодекс Российской Федерации об административных праовнарушениях и Федеральный закон от 21 июля 2014 года № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях». Оба принятых закона требуют осуществлять физическое размещение чувствительной для государственных органов и рядовых граждан информации в пределах государственных границ Российской Федерации. Результатом принятия данных законов должно стать существенное затруднение злонамеренных нарушений работы привычных для россиян интернет-сервисов из-за заграницы и общее повышение надёжности представляемых дистанционно государственных и частных услуг.
Другим важным направлением работы Комитета в 2013-2015 годах стала защита авторских прав. В результате многоступенчатой процедуры принятия Федерального закона от 24 ноября 2014 года № 364-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и Гражданский процессуальный кодекс Российской Федерации была постепенно отработана процедура досудебного урегулирования споров по авторским правам и внедрена система пресечения незаконного, «пиратского» использования практически всех видов содержания электронных коммуникационных сетей (за исключением фотографий). Созданная в ходе длительного обсуждения со всеми заинтересованными сторонами система позволяет урегулировать отношения между интернет-сообществом и правообладателями до момента наложения судебных санкций. При этом важным является полное исключение из закона каких-либо мер наказания против обычных потребителей нелегального контента.
С 2014 года при Комитете работает экспертный совет, в котором представлены все заинтересованные в реальном сотрудничестве с законодательной властью сегменты информационной отрасли. Кроме профессиональных ассоциаций, редакций СМИ, компаний работающих в сфере связи, информации и информационных технологий в совете представлены и организации гражданского общества. В частности с Комитетом сотрудничает Институт развития Интернета, располагающий возможностями эффективного взаимодействия со всеми ветвями власти и любыми сегментами современной электронной экономики.
Работа Комитета направлена на обеспечение развития экономики страны с применением передовых инфокоммуникационных решений, повышение эффективности государственного управления при обеспечении безопасности в информационном обществе, устранение цифрового неравенства регионов, повышение качества жизни граждан и улучшение условий развития бизнеса в информационном пространстве. Отмечу, что правовое обеспечение в сфере инфокоммуникационных технологий требует постоянного системного анализа всего комплекса вопросов правового регулирования. Поэтому

рассчитываем и на ваш вклад в постановку и решение значимых вопросов инфосферы. Это особенно важно, в связи с выработкой и реализацией стратегии развития информационного общества в Российской Федерации.

2. Экспериментальный раздел

Вопросы безопасности информации – важная часть процесса внедрения новых информационных технологий во все сферы жизни общества. Широкомасштабное использование вычислительной техники и телекоммуникационных систем в рамках территориально-распределенных ИС, переход на этой основе к безбумажной технологии, увеличение объемов обрабатываемой информации и расширение круга пользователей приводят к качественно новым возможностям несанкционированного доступа к ресурсам и данным информационной системы, к их высокой уязвимости.

Реализация угроз несанкционированного использования информации наносит сейчас гораздо больший ущерб, чем, например, «случайные» пожары в помещениях или физическое воздействие на сотрудников. Однако затраты на построение системы защиты информации еще пока несоизмеримо малы по сравнению с затратами на защиту от грабителей или на противопожарную защиту. Ктому же в современном бизнесе наблюдается постепенный переход от чисто физических методов воздействия на конкурентов к более интеллектуальным, в том числе с использованием новейших средств и способов добывания информации.

В настоящее время не существует единого определения термина «информация». С точки зрения различных областей знания данное понятие описывается своим специфическим набором признаков. Например, «информация» может трактоваться как совокупность данных, зафиксированных на материальном носителе, сохраняемых и распространяемых во времени и пространстве.

Угрозы безопасности информации выявляются путем поэтапного исследования:

1) технологии работы с конфиденциальными сведениями на защищаемомобъекте с целью определения всех основных носителей информации;

2) физических особенностей носителей информации, выявленных на первом этапе для определения спектра порождаемых ими паразитных носителей;

3) условий, при которых возможен перенос информации с носителей, имеющих место в системе, к злоумышленнику и обратно. При этом исследуются также и объекты, не имеющие прямого отношения к обработке информации, обладающие свойством принимать и передавать информацию (например, конструктивные элементы здания, бытовая электротехника и т.д.).

По результатам анализа технологии работы с информацией определяются носители информации, задействованные от момента поступления информации в систему до получения её потребителем. Выявление носителей информации целесообразно вести методом структурного поиска. Например, если в информационном обмене задействованы технические средства обработки, хранения или передачи информации, то сначала создается полный список таких технических средств, а затем анализируются носители- информации, присущие конкретному техническому средству (линии и узлы связи, оперативная память, видеопамять ЭВМ, магнитные или оптические накопители данных, средства отображения информации и т.д.).

В результате такого анализа появляется полный перечень функционально значимых носителей информации, задействованных в исследуемой системе. Выявленные носители информации исследуются с целью определения множества порождаемых ими паразитных носителей, затем формируется полный перечень носителей информации, которыми может воспользоваться злоумышленник. При этом вероятность использования канала доступа к информации, а соответственно и приоритетность внедрения мер защиты, будет зависеть от технических возможностей злоумышленника, его квалификации, соотношения: «стоимость использования канала – ценность добываемой информации», «пропускной способности» канала утечки и т.д. Рассмотренный подход применим к решению задачи выявления каналов возможного неправомерного доступа к информации на объекте информатики.

Органы государственной власти имеют дело с такими видами информации, как служебная тайна и персональные данные, которые в соответствии с Указом Президента РФ от 06.03.1997 № 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера», относятся к сведениям конфиденциального характера. Следовательно, в соответствии с законодательством РФ, органы государственной власти должны принимать меры по защите такой информации от разглашения, утечки по техническим каналам и несанкционированного доступа посредством организационно-правовых, инженерно-технических, криптографических мер. Защита информации – прямая обязанность

государственных органов, но при этом именно в госорганах доля утечек по всему миру, и в России в том числе, остается стабильно высокой. Построение и внедрение системы защиты информации (СЗИ) в целом является трудоёмкой задачей, так как на этапе разработки требуется отследить все взаимосвязи между процессами управления информационной безопасностью (ИБ), а также сконструировать большое количество процессов таким образом, чтобы они заработали эффективно.
Проблемы, препятствующие внедрению системы защиты информации и её эффективному функционированию, можно разделить на три уровня:
- правовые;
- организационные;
- технические.
При этом необходимо учитывать, что данные уровни взаимно влияют друг на друга. Первый уровень – правовой. Он связан с соблюдением этических и юридических норм при передаче и обработке информации. Российское законодательство в области защиты информации и персональных данных подчиняется общим принципам законодательства в любой области, а значит можно установить следующую иерархию нормативных правовых актов:
1. Федеральные законы.
2. Указы Президента.
3. Постановления Правительства.
4. Акты регуляторов.
Основными регуляторами в области защиты информации и персональных данных являются Федеральная служба по техническому и экспортному контролю России и Федеральная служба безопасности России. Уполномоченным органом по защите прав субъектов персональных данных является Федеральная служба по

Список использованной литературы
1. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 № Пр-1895) 2. Указ Президента РФ от 06.03.1997 № 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера» 3. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 21.07.2014) «О персональных данных»
2. Авсянников Н.М. Инновационный менеджмент: учебное пособие. - М.: РУДН, 2011. - 189 с.
3. Бышок А. С. Создание благоприятного инвестиционного климата с целью привлечения иностранного капитала [Текст] / А. С. Бышок, А. В. Дорофеева // Экономика, управление, финансы: материалы междунар. науч. конф. (г. Пермь, июнь 2011 г.). — Пермь: Меркурий, 2011. — С. 22-25.
4. Вертакова Ю.В., Симоненко Е.С. Управление инновациями: теория и практика: учеб. пособие. – М.: ЭКСМО, 2008. – 432 с.
5. Гапоненко А.Л., Панкрухин А.П. Стратегическое управление: учеб. для студентов вузов. – М.: Омега-Л, 2008. – 464 с.
6. Климанова А. П. Роль инноваций в обеспечении конкурентоспособности предприятий машиностроения/А. П. Климанова // Молодой ученый. — 2014. — №3. — С. 441-443.
7. Кокурин Д.И. Инновационная деятельность. - М.: Экзамен. 2001. – 576 с.
8. Курило А. П., Милославская Н. Г., Сенаторов М. Ю., Толстой А. И. Основы управления информационной безопасностью, учеб. пособ. для вузов. – 2-е изд., испр. – М.: Горячая линия- Телеком, 2014. – 244 с.: ил. – Серия «Вопросы управления информационной безопасностью. Выпуск 1»
9. Милославская Н. Г., Сенаторов М. Ю., Толстой А. И. Технические, организационные и кадровые аспекты управления информационной безопасностью, учеб. пособ. для вузов. – 2-е изд., испр. – М.: Горячая линия-Телеком, 2014. – 214 с.: ил. – Серия «Вопросы управления информационной безопасностью. Книга 4»
10. Мазур И.И. [и др.] Управление проектами: учебное пособие / Под общ. ред. И. И. Мазура и В. Д. Шапиро. – 6-е изд., стер. – М.: Издательство Омега-Л, 2010. – 960 с. – С.18.
11. Макаркин Н.Р., Шаворина Л.В. Инновационный менеджмент: Учебное пособие. – Саратов: Изд-во СГУ, 1997.
12. Медынский В.Г. Инновационный менеджмент: учебник. - М.: ИНФРА, 2008. - 295 с.
13. Миронова Н.Б. Инновационное развитие России: анализ основных индикаторов // Современные научные исследования и инновации. – Май 2013. - № 5 [Электронный ресурс]. URL: http://web.snauka.ru/issues/2013/05/24170 (дата обращения: 25.05.2014)
14. Пармон В.Н., Носков А.С., Анфимова Н.П.. Проблемы инновационного взаимодействия российской науки и

крупных производящих структур // Инновации. - №05. - 2014.
15. Фласинский М. Управление информационными проектами / пер. с польск. И. Д. Рудинского. – М.: Горячая линия-Телеком, 2013. – 190 с.