

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Локтионова Оксана Геннадьевна
Должность: проректор по учебной работе
Дата подписания: 15.02.2021 13:50:24
Уникальный программный ключ:
0b817ca911e6668abb13a5d426d39e5f1c11eabbf73e943df4a4851fda56d089

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)
Кафедра информационных систем и технологий

УТВЕРЖДАЮ
Проректор по учебной работе
О.Г. Локтионова
«15» 12 2020



**ДОКЛАДЫ ПО ТЕМАМ РАЗДЕЛА: "ПРАВОВЫЕ АСПЕКТЫ
ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ"**

методические указания по выполнению практической работы №3
по дисциплине «Информационные технологии»
для направления подготовки 10.05.02 Информационная
безопасность телекоммуникационных систем

Курск -2020

УДК 004

Составитель: Л.В. Стародубцева

Рецензент

Кандидат технических наук, доцент *Ю.А. Халин*

Доклады по темам раздела: "Правовые аспекты использования информационных технологий и программного обеспечения": методические указания по выполнению практической работы №3 / Юго-Зап. гос. ун-т; сост.: Л.В. Стародубцева. - Курск, 2020. 9 с.

Содержит теоретические сведения по дисциплине «Информационные технологии».

Методические указания по структуре, содержанию и стилю изложения материала соответствуют методическим и научным требованиям, предъявляемым к учебным и методическим пособиям.

Предназначены для студентов направления подготовки 10.05.02 Информационная безопасность телекоммуникационных систем

Текст печатается в авторской редакции

Подписано в печать *18.12.20*. Формат 60x84 1/16.
Усл.печ.л. *0,5*. Уч.-изд. л. *0,4*. Тираж *100* экз. Заказ. *408*
Бесплатно.

Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Практическая работа №3

Доклады по темам раздела: "Правовые аспекты использования информационных технологий и программного обеспечения"

Теоретические сведения

В Концепции национальной безопасности Российской Федерации определены важнейшие задачи в информационной сфере, в том числе и в правовой области:

- установление необходимого баланса между потребностью в свободном обмене информацией и допустимыми ограничениями ее распространения;

- разработка нормативной правовой базы и координация деятельности федеральных органов государственной власти и других органов, решающих задачи обеспечения информационной безопасности при ведущей роли Федерального агентства правительственной связи и информации при Президенте Российской Федерации.

Законодательство России в области информатизации начало формироваться с 1991 года.

Основополагающим понятием в области правового обеспечения является **информация**.

Закон РФ "Об информации, информатизации и защите информации" определяет понятие **информация** как "сведения о

лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления”.

При решении организационно-правовых вопросов обеспечения информационной безопасности исходят из того, что информация подпадает под нормы вещного права, что дает возможность применять к информации нормы Уголовного и Гражданского права в полном объеме.

Впервые в правовой практике России информация как объект права была определена в ст. 128, ч. 1, принятого в ноябре 1994 г. ГК РФ, где говорится: “К объектам гражданских прав относятся ...информация; результаты интеллектуальной деятельности, в том числе исключительные права на них (интеллектуальная собственность)...”. Данная статья дает возможность квалифицировать посягательства на сохранность и целостность информации, как преступления против собственности.

Этим же Законом определено, что **информационные ресурсы**, т. е. отдельные документы или массивы документов, в том числе и в информационных системах, являясь объектами отношений физических, юридических лиц и государства, подлежат обязательному учету и защите как материальное имущество собственника (ст.4.1,ст.6.1.). При этом собственнику предоставляется право самостоятельно в пределах своей компетенции устанавливать режим защиты информационных ресурсов и доступа к ним (ст.6.7).

Законодательные меры

Законодательные меры занимают около 5% объема средств, расходуемых на защиту информации. Это меры по разработке и практическому применению законов, постановлений, инструкций и правил эксплуатации, контроля как аппаратного, так и программного обеспечения компьютерных и информационных систем, включая линии связи, а также все объекты инфраструктуры, обеспечивающие доступ таким системам. В России деятельность в информационной сфере регулируют более 1000 нормативных документов. Уголовное преследование за преступления в этой сфере осуществляется в соответствии с гл. 28 Уголовного кодекса РФ «Преступления в сфере компьютерной информации», содержащей три статьи.

1. Ст. 272 - несанкционированный доступ к информации. ***Несанкционированный доступ к информации - нарушение установленных правил разграничения доступа с использованием штатных средств, предоставляемых ресурсами вычислительной техники и автоматизированными системами (сетями).***

Отметим, что при решении вопроса о санкционированное доступа к конкретной информации необходимо наличие документа об установлении правил разграничения доступа, если эти правила не прописаны законодательно.

2. Ст. 273 - создание, использование и распространение (включая продажу зараженных носителей) вредоносных программ для ЭВМ, хотя перечень и признаки их законодательно не закреплены. Вредоносная программа - специально созданная или

измененная существующая программа, заведомо приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ или их сети.

3. Ст. 274 - нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Это нарушение работы программ, баз данных, выдача искаженной информации, а также нештатное функционирование аппаратных средств и периферийных устройств; нарушение нормального функционирования сети, прекращение функционирования автоматизированной информационной систем в установленном режиме; сбой в обработке компьютерной информации.

Уголовное преследование за незаконные действия с общедоступной информацией осуществляется в соответствии со ст. 146 «Нарушение авторских и смежных прав» и 147 «Нарушение изобретательских и патентных прав» гл. 19 «Преступления против конституционных прав и свобод человека и гражданина» Уголовного кодекса РФ.

Ответственность за соблюдением сотрудниками организации или компании законодательных мер по защите информации лежит на каждом сотруднике организации или компании, а контроль за их соблюдением - на руководителе.

В существующей практике можно выделить следующие основные аспекты решения проблемы защиты информации:

- анализ правового обеспечения;
- реализация организационно-правовых мероприятий защиты;

- реализация технических мероприятий по защите информации.

Комплексное изучение установленных норм и правил в конкретной прикладной области всегда является обязательным элементом культуры работающего в этой области специалиста.

Анализ правового обеспечения планируемых к осуществлению мероприятий в области организации защиты информации всегда должен предшествовать принятию окончательного решения о реализации этих мероприятий.

К организационно-правовым мероприятиям по защите конфиденциальной информации относятся мероприятия по разработке и принятию определенных документов предприятий и организаций, регламентирующих степень и порядок допуска собственных сотрудников, а также сторонних лиц и организаций к конкретным информационным ресурсам.

Организационно-правовая защита информации реализуется путем установления на предприятии режима конфиденциальности. Можно выделить три формы конфиденциальных отношений:

- Между сотрудником предприятия и самим предприятием как юридическим лицом. Реализуется на практике путем составления соответствующего трудового договора или контракта, заключаемого с сотрудником предприятия.

- Складывающиеся между конкретным сотрудником и другими сотрудниками этого предприятия. Эти отношения развиваются как по вертикали, так и по горизонтали. Указанные отношения называются конфиденциальными отношениями по служебным функциям. Юридически эти отношения закрепляются

многообразными административно-правовыми решениями, например приказами о выполнении определенных работ, и регламентируются “Должностными инструкциями”.

· Складывающиеся в рамках хозяйственных работ и базирующиеся на договоре между партнерами. Юридически конфиденциальные отношения закрепляются в виде четко сформулированных требований и обязательств, которые выдвигают договаривающиеся стороны, и фиксируются в договоре.

В вопросах реализации технических мероприятий обеспечения информационной безопасности с точки зрения правового обеспечения основное внимание следует уделять выполнению требований лицензирования исполнителей работ и использования сертифицированных средств защиты, а также действующим ограничениям на применение специальных технических средств.

Основными проблемы правового обеспечения информационной безопасности являются:

Защита прав на получение информации - предполагает обеспечение условий, препятствующих преднамеренному сокрытию или искажению информации при отсутствии для этого законных оснований. В соответствии со ст.29 Конституции РФ, “Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом”.

Задание

Найдите в сети Интернет “Федеральный закон об информации, информационных технологиях и о защите информации”, изучите его. Ответьте на вопросы:

- Сколько статей содержит данный закон?
- С какой целью создан данный закон?
- Перечислите основные понятия, которые вы встретили в законе?
- Какие виды информации в зависимости от распространения вам известны?
- Права обладателя информации?
- Как защитить информацию?
- Какую ответственность несет нарушение этого закона?