УВАЖАЕМЫЕ СТУДЕНТЫ! Законспектируйте в своей рабочей тетради по дисциплине приведенную лекцию (объемом 4-5 страницы), ответьте *письменно* на контрольные вопросы.

Результаты работы, фотоотчет, предоставить преподавателю на e-mail: igor-gricenko-95@mail.ru в течении ТРЕХ дней.

При возникновении вопросов по приведенному материалу обращаться по следующему номеру телефона: (072)132-63-42

ВНИМАНИЕ!!! При отправке работы, не забывайте указывать ФИО студента, наименование дисциплины, дата проведения занятия (по расписанию).

Тема 1.4: Правовые нормы, относящиеся к информации, правонарушения в информационной сфере, меры их предупреждения. Электронное правительство.

План

1. Правовые нормы, относящиеся к информации, правонарушения в информационной сфере, меры их предупреждения.
2. Электронное правительство**.**

1. Правовые нормы, относящиеся к информации, правонарушения в информационной сфере, меры их предупреждения

Первоначально информация находится в памяти человека, а чтобы избежать потерь, переносится на материальные носители: книги, диски, кассеты и прочие накопители, предназначенные для хранения информации. Как следствие, информация может тиражироваться путем распространения материального носителя. Перемещение такого материального носителя от субъекта-владельца, создающего конкретную информацию, к субъекту-пользователю влечет за собой утрату права собственности у владельца информации.

Интенсивность этого процесса существенно возросла в связи с тотальным распространением сети Интернет. Ни для кого не секрет, что очень часто книги, музыка и другие продукты интеллектуальной деятельности человека безо всякого на то согласия авторов или издательств размещаются на различных сайтах без ссылок на первоначальный источник. Созданный ими интеллектуальный продукт становится достоянием множества людей, которые пользуются им безвозмездно, и при этом не учитываются интересы тех, кто его создавал.

Принимая во внимание, что информация практически ничем не отличается от другого объекта собственности, например машины, дома, мебели и прочих материальных продуктов, следует говорить о наличии подобных же прав собственности и на информационные продукты. Право собственности состоит из трех важных компонентов: права распоряжения, права владения и права пользования.

Преступления в сфере информационных технологий включают как распространение вредоносных вирусов, взлом паролей, кражу номеров кредитных карточек и других банковских реквизитов (фишинг), так и распространение противоправной информации (клеветы, материалов порнографического характера, материалов, возбуждающих межнациональную и межрелигиозную вражду и т.п.) через Интернет, коммунальные объекты.

Кроме того, одним из наиболее опасных и распространенных преступлений, совершаемых с использованием Интернета, является мошенничество.

Так, в Российской Федерации принят ряд указов, постановлений, законов, таких как:

1. «Об информации, информатизации и защите информации»,
2. «Об авторском праве и смежных правах»,
3. «О правовой охране программ для ЭВМ и баз данных»,
4. «О правовой охране топологий интегральных схем» и т. д.».

Меры обеспечения информационной безопасности

Основные виды преступлений, связанных с вмешательством в работу компьютеров:

1. Несанкционированный доступ к информации, хранящейся в компьютере. Несанкционированный доступ осуществляется, как правило, с использованием чужого имени, изменением физических адресов технических устройств, использованием информации оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных.
2. Ввод в программное обеспечение «логических бомб», которые срабатывают при выполнении определённых условий и частично или полностью выводят из строя компьютерную систему.
3. Разработка и распространение компьютерных вирусов.
4. Преступная небрежность в разработке, изготовлении и эксплуатации программно-вычислительных комплексов, приведшая к тяжким последствиям.
5. Подделка компьютерной информации.

6. Хищение компьютерной информации.

2. Электронное правительство

Предупреждение компьютерных преступлений
При разработке компьютерных систем, выход из строя или ошибки в работе которых могут привести к тяжёлым последствиям, вопросы компьютерной безопасности становятся первоочередными. Известно много мер, направленных на предупреждение преступления:
Организационные:
1. Повышение квалификации персонала,
2. Контролируемые каналы распространения информации,
3. Разделение прав доступа, уничтожение ненужных копий документов,
4 Соблюдение коммерческой тайны персоналом.
5Охрана вычислительного центра,
6. Тщательный подбор персонала,
7. Исключение случаев ведения особо важных работ только одним человеком,
8. Наличие плана восстановления работоспособности центра после выхода его из строя,
9. Организация обслуживания вычислительного центра посторонней организацией или лицами, незаинтересованными в сокрытии фактов нарушения работы центра,
10. Универсальность средств защиты от всех пользователей (включая высшее руководство),
11. Возложение ответственности на лиц, которые должны обеспечивать безопасность центра.
Юридические
1. Разработка норм, устанавливающих ответственность за компьютерные преступления,
2. Защита авторских прав программистов,
3. Совершенствование уголовного, гражданского законодательства и судопроизводства.
4. общественный контроль за разработчиками компьютерных систем и принятие международных договоров об ограничениях, если они влияют или могут повлиять на военные, экономические и социальные аспекты жизни стран, заключающих соглашение.
В России действуют: Закон «О правовой охране программ для ЭВМ и баз данных» и Закон «Об авторском праве и смежных правах».

Уголовный Кодекс содержит статьи:
Ст. 272 «О неправомерном доступе к компьютерной информации»
Ст. 273 «Создание, использование и распространение вредоносных программ для ЭВМ»
Ст. 274 «Нарушение правил эксплуатации ЭВМ, систем ЭВМ или сети ЭВМ»
Программно-технические.
1 Защита от компьютерных вирусов;
2. Шифрование данных;
3. Резервное копирование данных;
4. Ограничение доступа к устройствам и файловой системе;
5. Контроль трафика с помощью межсетевых экранов (брандмауэров);
6. Защита от несанкционированного доступа к системе;
7. Резервирование особо важных компьютерных подсистем;
8. Организация вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев,
9. Установка оборудования для обнаружения и тушения пожара, оборудования для обнаружения воды;
10. Принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установка резервных систем электропитания,
11. Оснащение помещений замками, установку сигнализации и многое другое.
Результаты опроса представителей служб безопасности 492 компаний, дает представление о наиболее опасных способах совершения компьютерных преступлений.
Наивысшая угроза. Виды атак, выявленные за последние 12 месяцев:
1. Вирус 83%
2. Злоупотребление сотрудниками компании доступом к Internet 69%
3. Кража мобильных компьютеров 58%
4. Неавторизованный доступ со стороны сотрудников компании 40%
5. Мошенничество при передаче средствами телекоммуникаций 27%
6. Кража внутренней информации 21%
7. Проникновение в систему 20%

Вопросы для самоконтроля
1. Что является преступлением в сфере информационных технологий?
2. Приведите примеры преступлений в сфере информационных технологий.
3. Назовите меры, направленные на предупреждение преступления в сфере информационных технологий. Какими законами, постановлениями эти меры регламентированы?