Организационное и правовое обеспечение информационной безопасности

Доцент кафедры БИТ

к.т.н. **Струков Владимир Ильич**

Вопросы по теме 4 (4.1. 4.2.)

1. Какую информацию относят к сведениям, составляющим КТ?

2. Виды конкурентной разведки.

3. Отличие конкурентной разведки от промышленного шпионажа.

4. Кокой закон регулирует отношения по защите КТ?

5. Сведения, которые не могут составлять КТ.

6. Что значит ввести режим КТ на предприятии?

7. Ответственность за разглашение информации, содержащей КТ.

4. Правовая защита коммерческой тайны
4.3. Правовое регулирование отношений по защите КТ на предприятии

В соответствии с установленными законом о КТ на предприятии используются правовые нормы внутрифирменных документов для регулирования правовых отношений по защите КТ.

Такими документами являются:

1.Устав предприятия;
2.Коллективный договор предприятия;
3.Трудовые и гражданско-правовые договора;
4.Правила внутреннего трудового распорядка рабочих и служащих предприятия;
5.Должностные обязанности руководителей, специалистов, рабочих и служащих предприятия.
и другие документы.

Для создания правовых основ защиты информации на коммерческом предприятии необходимо:

1.Ввести в Устав предприятия в раздел “Права и обязанности предприятия”:

“Предприятие имеет право определять состав, объем и порядок защиты сведений, составляющих КТ, требовать от сотрудников предприятия обеспечения ее сохранности”.

“Предприятие обязано обеспечить сохранность КТ”.

Внесение этих требований дает право администрации предприятия:

-создавать организационные структуры по защите КТ;

-издавать нормативные и распорядительные документы, определяющие порядок выделения сведений, составляющих КТ, и механизмы ее защиты;

-включать требования по защите КТ в договора по всем видам хозяйственной деятельности;

-требовать защиту интересов предприятия перед государственными и судебными органами.

2.Разработать **“Перечень сведений, составляющих КТ предприятия”** и довести его под роспись до всех сотрудников.

3.Дополнить “Коллективный договор” следующими требованиями:

В раздел “Предмет договора”

Администрация предприятия обязуется обеспечить разработку и осуществление мероприятий по введению режима и защите КТ.

Трудовой коллектив принимает на себя обязательство по соблюдению установленных на предприятии требований по защите КТ.

В раздел “Кадры”

Администрация обязуется привлекать нарушителей требований по защите КТ к административной и уголовной ответственности в соответствии с действующим законодательством.

4.Дополнить правила внутреннего распорядка дня работников требованиями о неразглашении КТ.

При поступлении рабочего или служащего на работу, переходе его на другую работу а также при увольнении, администрация обязана проинструктировать работника по правилам сохранения КТ с оформлением письменного обязательства о ее неразглашении.

5.Ввести в текст трудового договора требования по защите КТ.

Тогда независимо от формы заключения договора (устная или письменная) подпись работника на приказе о приеме на работу подтверждает его согласие с условиями договора.

Если договор заключается в устной форме, то действует требование по защите КТ, вытекающее из правил внутреннего трудового распорядка.

6.В должностные обязанности руководителей, специалистов, рабочих и служащих записать, что:

-сотрудники должны знать относящиеся к их деятельности сведения, являющиеся КТ, выполнять лично требования по ее защите и принимать меры по предупреждению нарушений установленных норм сохранности КТ.

Включение этих требований дает право администрации предприятия применять к нарушителям меры дисциплинарного воздействия в соответствии с Трудовым кодексом РФ.

Руководителю предприятия, при создании системы безопасности на своей фирме, необходимо определить следующее:

-какая информация нуждается в защите;

-кого она может заинтересовать;

-каков “срок жизни” этих секретов;

-во что обойдется их защита.

В рамках режима КТ на предприятии вводятся система закрытого делопроизводства, которая включает:

1. Создание отдела защищенного делопроизводства.

2. Проведение документирования:

-определение перечня документов, содержащих секреты предприятия;

-контроль за содержанием документов и степени секретности;

-контроль за размножением и рассылкой документов;

-учет документов с грифом “КТ” (производится отдельно от несекретных документов и документов ДВИ) включает:

-регистрация каждого вх. и исх. документа;

-инвентарный учет;

-номенклатуру дел, журналов и карточек;

-контроль за местоположением документов.

Корреспонденция с грифом “КТ” поступает в ОЗД, где она проверяется на наличие недостачи и регистрируется на корточках или в журнале.

Листы журналов нумеруются, прошиваются и опечатываются.

На первом листе зарегистрированного входящего документа с грифом “КТ” ставится штамп

Наименование предприятия		
Входящий № и дата	**Количество листов**	
	основных	**приложений**

Исходящие документы с грифом “КТ” печатаются в машбюро ОЗД или с учтенных носителей с помощью средств ВТ.

На последнем листе каждого экземпляра проставляется количество отпечатанных экземпляров, фамилия исполнителя, машинистки и дата.

Отпечатанный документ регистрируется в журнале.

Все черновики выполняются на предварительно учтенных в ОЗД листах, сдаются после окончания работы и уничтожаются в ОЗД.

Отправка документов с грифом “КТ” производится заказными письмами или бандеролями.

При этом рекомендуется использовать двойной конверт, причем, на внешнем пишется адрес, а на внутреннем ставится гриф.

Проверка наличия документов проводится

ежеквартально- для документов, находящихся на исполнении

ежегодно- для всех зарегистрированных документов.

Режимные документы, находящихся у сотрудников на исполнении, хранятся на предприятии в опечатанных папках или чемоданах .

3. Организацию документооборота:

-установление разрешительной системы доступа исполнителей к документам;

-установление грифа секретности (степени секретности);

-установление порядка приема передачи документов между сотрудниками;

-контроль за порядком работы с документами;

-установление порядок хранение и уничтожение документов;

-установление порядка обращения с документами.

Порядок хранение и уничтожение документов включает:

-выделение специально оборудованных помещений;

-установление порядка доступа к делам;

-контроль за своевременностью и правильностью формирования дел;

-установление порядка подготовки документов для уничтожения;

-обеспечение необходимых условий уничтожения;

-контроль за правильностью и своевременностью уничтожения документов.

Порядок обращения с документами

1.Выдача документов с грифом КТ сотрудникам производится по разрешению руководителя предприятия на основании служебной записки от начальника подразделения исполнителя.
2.Передача документов с грифом “КТ” между сотрудниками осуществляется под расписку и в пределах круга лиц, допущенных к данному документу.
3.После окончания рабочего дня помещения ОЗД передаются под охрану.
4.Разрешение на уничтожение документа дает руководитель подразделения, к деятельности которого относится документ, путем записи в журнал учета «Уничтожить», подпись, дата.
5.Уничтожение документов производится путем их сожжения или измельчения.

4.4. Защита коммерческой информации в договорной документации

Правовая защита коммерческих секретов, основывается на использовании таких внутрифирменных нормативных документов как **трудовой договор** (контракт) и **должностные инструкции.**

Содержанием трудового договора являются взаимные права и обязанности и установлена ответственность при исполнении должностных инструкций.

В трудовом договоре принято различать **основные** (законодательно определенные) и **дополнительные** (факультативные) условия.

Вопросы защиты информации закрепляются в трудовом договоре в виде **дополнительных условий**.

В обязанности работника включают условие о неразглашении служебной (коммерческой) тайны, к которой он будет допущен в силу его должностных обязанностей.

Кроме трудового договора данное условие может быть также включено и в другие виды договоров:

-договор поручительства;

-договор коммерческого представительства;

-агентский договор;

-договор поручения или доверенности;

-договор о рекламных услугах;

-другие информационные услуги.

В этих документах включаются следующие обязательства:

-не разглашать КТ организации третьим лицам или публично без согласия администрации;
-сохранять КТ тех организаций, с которыми имеются деловые связи;
-выполнять требования приказов и инструкций по защите КТ предприятия;
-не использовать секретные сведения организации, занимаясь другой деятельностью (ущерб от конкурентного действия);
-незамедлительно извещать СБ о попытках посторонних лиц получить закрытую информацию;
-незамедлительно извещать об утрате носителей секретной информации и другие факты нарушения режима ее защиты;
-при увольнении все носители КТ с которыми работал сотрудник передаются соответствующему должностному лицу;
-предупреждение работника о наступлении гражданской, административной или уголовной ответственности в случае нарушения взятых обязательств.

Обязанности по сохранению КТ возлагаются и на руководителя организации.

Для этого в контракт, заключаемый с руководителем вводятся соответствующие положения:

-обязательство руководителя хранить КТ и не использовать ее в ущерб организации;

-о персональной ответственности за создание необходимых условий для сохранности КТ;

-об ответственности руководителя за нарушения режима защиты КТ и возможных последствиях.

Защита прав обладателя коммерческих секретов осуществляется способами, предусмотренными также ГК РФ и другими законами.

Среди них можно выделить следующие:

пресечение действий, нарушающих право или создающих угрозу его нарушения;

возмещение убытков, в том числе и упущенной выгоды (ГК РФ ст. 12, 15).

Убыток - это выраженный в денежной форме ущерб, который состоит из затрат, связанных с созданием этих документов (например, стоимость бумаги) и упущенной выгоды, т.е. из доходов, которые могло бы получить предприятие в случае сохранения тайны.

4.5. Правовая защита от компьютерных преступлений

Средства автоматизированной обработки информации с использованием ЭВМ имеют ряд особенностей, дающих широкие возможности для злоумышленных действий.

Потери от КП во всем мире достигают в миллиарды долларов в год. Особенно страдают кредитно-финансовые учреждения.

Кроме этих действий значительные потери возникают в результате распространения вредоносных программ - компьютерных вирусов, появившиеся с 1987г.

Особенностью компьютерных преступлений является то, что их жертвы не всегда обращаются за защитой в правоохранительные органы (по коммерческим соображениям).

Можно выделить следующие
виды угроз информации в АС.

1.Перехват информации:

-по электромагнитному излучению (излучения ЭЛТ можно принимать на расстояниях до 1000 м.);

-по виброакустическому каналу (таблетки, клопы, жучки, через несущие конструкции и проемы здания, стетоскоп);

-видеоперехват (бинокль, фото- и видеокамеры);

-использование отходов информационного процесса (физические - дискеты, пленки и “мусор” в памяти компьютера).

2.Несанкционированный доступ (НСД) к информации:

-физическое проникновение;

-установка шлейфов;

-подключение к линии связи законного пользователя;

-подбор кода доступа в т.ч. с помощью программ- “взломщиков”, в ручную с помощью “интеллектуального” перебора - вскрывается 42% паролей из 8 символов.

3.Манипуляция данными и управляющими командами:

-умышленное изменение данных;

-изменение логических связей в электронных цепях и топологии микросхем.

4.Компьютерные вирусы.

“Троянский конь” - программа выдает себя за известную

“Троянская матрешка” - программа создает “троянского коня” и самоуничтожается.

“Троянский червь” - реализуется саморазмножения.

“Логическая бомба” - программа активируется при стечении определенных обстоятельств (включает алгоритм “троянского коня”) или в определенный момент времени “временная бомба”.

“Воздушный змей” переброска средств с одного счета на другой и обратно с постепенным увеличением сумм.

5.Использование специальных программных средств:

-“моделирование” процессов и способов преступления путем создания игровой программы **защита-преодоление**.

6.Комплексные методы.

Использование двух и более способов и их комбинации.

Эффективная борьба с КП в РФ ведется с 1997г. после принятия УК РФ, в котором помещена глава 28 «Преступления в сфере компьютерной безопасности».

Составы компьютерных преступлений даны в следующих статьях:

-«Неправомерный доступ к компьютерной информации» (ст. 272);

-«Создание, использование и распространение вредоносных программ для ЭВМ» (ст. 273);

-«Нарушение правил эксплуатации ЭВМ» (ст. 274).

Статья 272. Неправомерный доступ к компьютерной информации

1. **Неправомерный доступ к компьютерной информации**, то есть информации на машинном носителе, в ЭВМ, системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, или их сети, -

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, **либо лишением свободы на срок до двух лет**.

2. **То же деяние, совершенное организованной группой** либо лицом с использованием своего служебного положения, имеющим доступ к ЭВМ,-

наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, **либо лишением свободы на срок до пяти лет.**

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами -

наказываются лишением свободы на срок до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, - наказываются лишением свободы на срок от трех до семи лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

1. **Нарушение правил эксплуатации ЭВМ**, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, **если это деяние причинило существенный вред**, -

наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо **ограничением свободы на срок до двух лет.**

2. То же деяние, повлекшее по неосторожности тяжкие последствия, - наказывается лишением свободы на срок до четырех лет.

Целям защиты информации, обрабатываемой в АС служит принятый 2002 г.

Закон РФ «Об электронной цифровой подписи» (в ред ФЗ "Об электронной подписи" от 6 апреля 2011 г. N 63-ФЗ)

ЭЦП – реквизит документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе (ст. 3) **признается равнозначной собственноручной подписи лица на бумажном носителе, заверенном печатью** (ст. 19).

Контрольные вопросы

1. Какие внутрифирменные документы, использует предприятие для регулирования правовых отношений по защите конфиденциальной информации?

2. В какие виды договоров может быть также включено условие о неразглашении служебной (коммерческой) тайны?

3. Какими способами осуществляется защита прав обладателя коммерческой тайны?

4. Назовите виды угроз информации в автоматизированных системах?

5. Где указаны нормы ответственности за компьютерные преступления?