Лекция 11. Правовое обеспечение безопасности организации при использовании ИКТ-среды

Проф. Стрельцов Анатолий Александрович

Основные вопросы лекции

- 1. Понятие «организация»
- 2. Угрозы безопасности «организации» в ИКТ-среде
- 3. Некоторые правовые механизмы обеспечения безопасности «организации» в ИКТ-среде

Контрольный вопрос

- Основные угрозы безопасности «организации» в ИКТ-среде
- Правовые механизмы обеспечения безопасности «организации» при использовании ИКТ

1. Понятие «организация»

- Организация – единый, целостный и самостоятельно функционирующий и саморегулирующийся механизм, который имеет индивидуалистическую внутреннюю структуру, специфическое имущественное устройство, органы управления, формирующие и выражающие волю, которая не всегда совпадает с волей отдельного участника
- Юридическое лицо – организация, которая имеет в собственности, хозяйственном ведении или оперативном управлении обособленное имущество, может от своего имени приобретать и осуществлять имущественные и личные неимущественные права, нести ответственность, быть истцом и ответчиком в суде

Основные права организации в информационной сфере

- Право обладания информацией
- Право доступа к информации
- Право распространения информации
- Право создания и использования ИКТ-среды
- Право информационной безопасности (конфиденциальности)
- Источники права- № 149-ФЗ «Об информации, информационных технологиях и о защите информации», ГК РФ, № 395-1 ФЗ и другие

Особенности реализации прав организации в информационной сфере

- Права организации в информационной сфере неразрывно связаны (обусловлены) ее правовым статусом юридического лица (имеющего в хозяйственном ведении или оперативном управлении обособленное имущество и отвечающего по своим обязательствам этим имуществом, могущего от своего имени приобретать и осуществлять имущественные и личные неимущественные права, нести обязанности, быть истцом и ответчиком в суде), а также ее учредительными документами, закрепляющими порядок управления организацией.

2. Основные угрозы безопасности организации в ИКТ-среде

- Определение основных угроз безопасности организации в ИКТ-среде и противодействие им осуществляет сама организация. В то же время некоторые общественные отношения в области противодействия угрозам ИБ регулируются правом.
- К числу таких угроз, в частности, относятся:
- распространение без согласия организации информации, позволяющей ей при существующих или возможных обстоятельствах получать коммерческую выгоду;
- нарушение целостности электронных документов и их подписание неуправомоченными лицами

3. Основные источники права

- Основные источники права:
- № 149-ФЗ 27.07.2006 "Об информации, информационных технологиях и о защите информации»
- «Об электронной подписи»
- № 98-ФЗ от 29.07.2004 "О коммерческой тайне"

Правовые средства обеспечения безопасности организации в ИКТ-среде

- Правовой режим коммерческой тайны;
- Правовой институт электронной подписи

3.1. Правовой режим тайны

- Виды организаций:
- Коммерческие организации (хозяйственные товарищества и общества, включая кредитно-финансовые организации; производственные кооперативы; унитарные предприятия)
- Некоммерческие организации (потребительские кооперативы, общественные и религиозные организации, фонды, учреждения, объединения юридических лиц)

Правовой режим коммерческой тайны

- Коммерческая тайна – режим конфиденциальности информации, позволяющей ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.
-

Объект коммерческой тайны

- Информация, составляющая коммерческую тайну – сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны

Обладатель информации, составляющей коммерческую тайну

- Обладатель информации, составляющей коммерческую тайну,- лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны.
- Доступ к информации, составляющей коммерческую тайну, - ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации

Право отнесения информации к коммерческой тайне

- Право на отнесение информации к информации, составляющей коммерческую тайну, и на определение перечня и состава такой информации принадлежит обладателю такой информации с учетом положений законодательства Российской федерации.
- Информация, составляющая коммерческую тайну, полученная от ее обладателя на основании договора или другом законном основании, считается полученной законным способом.

Сведения, которые не могут составлять коммерческую тайну

- содержащиеся в учредительных документах;
- содержащиеся в документах, дающих право на осуществление предпринимательской деятельности;
- о составе имущества;
- о загрязнении окружающей среды;
- о численности, о составе работников, о системе оплаты труда, об условиях труда,
- обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

Права обладателя информации, составляющей коммерческую тайну

- устанавливать, изменять, отменять в письменной форме режим коммерческой тайны;
- использовать информацию, составляющую коммерческую тайну;
- разрешать или запрещать доступ к информации, составляющей коммерческую тайну;
- требовать от лиц, получивших доступ к информации, составляющей коммерческую тайну, соблюдения обязанностей по охране ее конфиденциальности

Охрана конфиденциальности информации

- Режим коммерческой тайны считается установленным после принятия обладателем информации, составляющей коммерческую тайну, установленных законодательством мер:
- определение перечня информации, составляющей коммерческую тайну;
- ограничение доступа к информации, составляющей коммерческую тайну,
- учет лиц, получивших доступ к информации;
- регулирование отношений с работниками и контрагентами;

Обязанности обладателя информации, составляющей коммерческую тайну

- В целях охраны конфиденциальности работодатель обязан:
- ознакомить под расписку работника: с перечнем информации, составляющей коммерческую тайну доступ к которой необходим для исполнения трудовых обязанностей; с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушение;
- создать работнику необходимые условия для соблюдения им установленного работодателем режима коммерческой тайны.
-

Техническая защита информации, составляющей коммерческую тайну

- Наряду с мерами, указанными в законодательстве, обладатель информации, составляющей коммерческую тайну, вправе применять при необходимости средства и методы технической защиты конфиденциальности этой информации, другие не противоречащие законодательству Российской Федерации меры

Достаточность мер по охране конфиденциальности

- Меры по охране конфиденциальности информации признаются разумно достаточными, если:
- исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя;
- обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны.
-

Обязанности работника

- выполнять установленный работодателем режим коммерческой тайны;
- 2) не разглашать эту информацию, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях;
- возместить причиненные работодателю убытки, если работник виновен в разглашении информации, составляющей коммерческую тайну
- передать работодателю при прекращении или расторжении трудового договора материальные носители информации, содержащие информацию, составляющую коммерческую тайну.

Охрана конфиденциальности информации при ее предоставлении

- Органы государственной власти обязаны создать условия, обеспечивающие охрану конфиденциальности информации, предоставленной им юридическими лицами или индивидуальными предпринимателями.
- Должностные лица органов государственной власти, иных государственных органов, органов местного самоуправления без согласия обладателя информации, составляющей коммерческую тайну, не вправе разглашать или передавать другим лицам.
- 3. В случае нарушения конфиденциальности информации должностными лицами органов государственной власти эти лица несут ответственность в соответствии с законодательством Российской Федерации.

Юридическая ответственность

- Нарушение норм федерального законодательства влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность
-

3.2. Правовой институт электронной подписи

- Правовой институт электронной подписи образуется совокупностью правовых норм, регулирующих общественные отношения в области создания и использования электронной подписи как средства реализации обычая делового оборота документов на бумажном носителе, подписываемых субъектами различных правоотношений собственноручной подписью и скрепляемых печатью организации.

Пример.

- Статья 60. Гарантии прав кредиторов реорганизуемого юридического лица
- (в ред. Федерального закона от 05.05.2014 N 99-ФЗ)
- 1. В течение трех рабочих дней после даты принятия решения о реорганизации юридического лица оно обязано уведомить в письменной форме уполномоченный государственный орган, осуществляющий государственную регистрацию юридических лиц, о начале процедуры реорганизации с указанием формы реорганизации.

Электронный документ

- Электронный документ - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах;
- Документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.
- .

Правовые средства реализации ЭП

- Электронная подпись и процедура ее применения – подтверждает волю субъекта, осуществляющего юридически значимое действие посредством подписания документа в письменной форме.
- Правовые статусы удостоверяющих центров, уполномоченных органов исполнительной власти - создают гарантии использования электронной подписи только уполномоченным субъектом, а также ограничения действия ЭП во времени и пространстве.

Принципы использования ЭП

- право участников электронного взаимодействия использовать ЭП по своему усмотрению, если требование об использовании конкретного вида электронной подписи в соответствии с целями ее использования не предусмотрено законодательством;
- возможность использования участниками электронного взаимодействия по своему усмотрению любой информационной технологии и (или) технических средств, позволяющих выполнить требования законодательства применительно к использованию конкретных видов электронных подписей;
- недопустимость признания ЭП и (или) подписанного ею электронного документа не имеющими юридической силы только на основании того, что такая ЭП создана не собственноручно, а с использованием средств электронной подписи для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе.

Электронные документы, подписываемые ЭП

- Простая ЭП – посредством использования кодов, паролей и иных средств подтверждает факт формирования ЭП определенным лицом.
- Информация, подписанная простой ЭП признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью.

Электронные документы, подписываемые неквалифицированной подписью

- Неквалифицированная подпись – ЭП, полученная в результате криптографического преобразования с использованием ключа ЭП; позволяет определить лицо, подписавшее документ; позволяет обнаружить факт внесения изменений в ЭД после подписания; создается с использованием средств ЭП.
- Информация, подписанная неквалифицированной ЭП признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью и заверенному печатью.

Электронные документы, подписываемые неквалифицированной подписью

- Квалифицированная ЭП – ЭП, соответствующая требованиям к неквалифицированной ЭП, а также дополнительно: ключ проверки ЭП указан в квалифицированном сертификате; средства ЭП имеют подтверждение требованиям законодательства
- Информация, подписанная квалифицированной ЭП, признается ЭД, равнозначным документу на бумажном носителе, подписанному собственноручной подписью и может применяться в любых правоотношениях, кроме случаев, когда требуется документ на бумажном носителе.

Удостоверяющий центр

- Удостоверяющий центр - юридическое лицо, индивидуальный предприниматель либо орган местного самоуправления, осуществляющий функции по созданию и выдаче сертификатов ключей проверки ЭП, средств ЭП, а также иные функции, предусмотренные федеральным законодательством.

Средства электронной подписи

- Средства ЭП позволяют при создании и проверке ЭП, создании ключа ЭП и ключа проверки ЭП:
- установить факт изменения подписанного документа после момента его подписания;
- обеспечить практическую невозможность вычисления ключа ЭП из ЭП или из ключа ее проверки.

Правовой статус уполномоченного федерального органа

- Осуществляет аккредитацию удостоверяющих центров, проводит проверки соблюдения аккредитованными удостоверяющими центрами требований, установленных законодательством, в том числе требований, на соответствие которым эти удостоверяющие центры были аккредитованы, и в случае выявления несоблюдения этих требований выдает предписания об устранении выявленных нарушений;
осуществляет функции головного удостоверяющего центра в отношении аккредитованных удостоверяющих центров.