О разрешительной системе доступа к информации, допустимых границах контроля и доверии работнику

Емельянников
Михаил Юрьевич,
Управляющий партнер

Знаете ли Вы, что защищаете?

- информация
- данные
- ресурсы
- сервисы

Какую информацию?

- информация ограниченного доступа
- чувствительная информация
- информация, необходимая для реализации бизнес-процессов
- информация, обязательная к раскрытию и опубликованию
- справочная информация

Что обеспечивает защита?

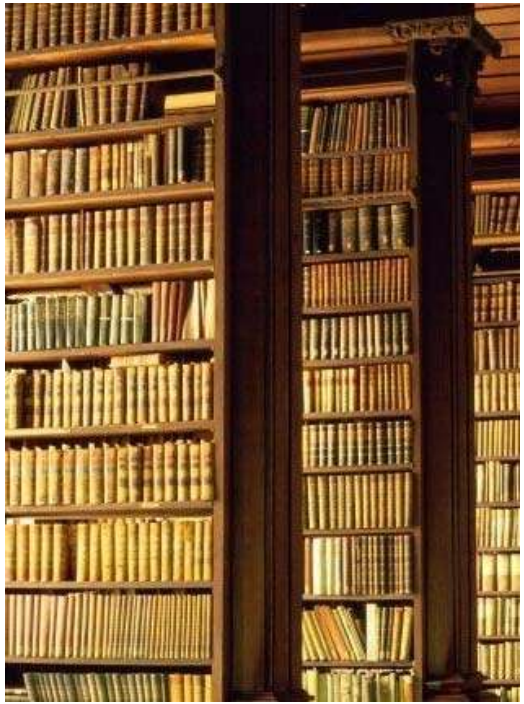
- конфиденциальность (информация ограниченного доступа и чувствительная информация
- целостность (данные, информация, необходимая для реализации бизнес-процессов, обязательная к раскрытию и опубликованию, справочная)
- доступность (ресурсы и сервисы, информация, необходимая для реализации бизнес-процессов…)

Когда все это можно защищать?

Информационные ресурсы, сервисы и информация:

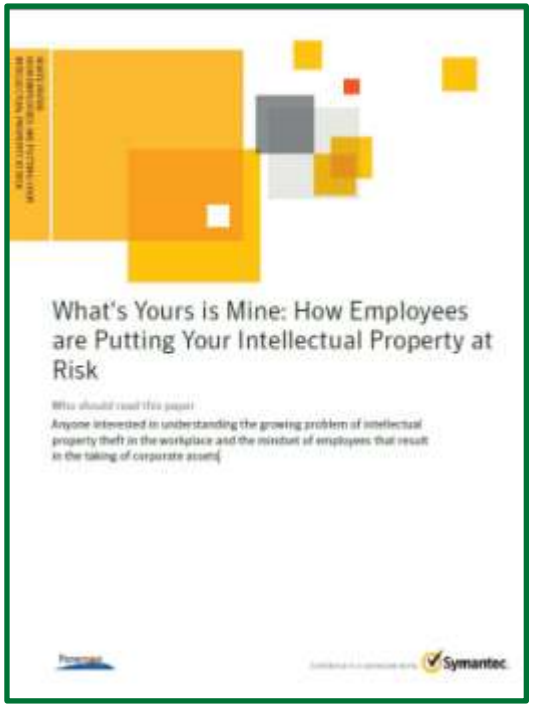
- систематизированы
- инвентаризованы
- категорированы (поименованы)

Для каждого ресурса определено ответственное за него лицо.



Вы полагаетесь на лояльность?

- 62% работников считают приемлемым перенос рабочих документов на личные компьютеры, планшеты, смартфоны, а также в онлайн-сервисы. Эта информация не удаляется, потому что работники не видят в ее хранении никакой опасности.
- 56% работников не считают преступлением использовать конфиденциальную информацию конкурентов.
- 51% считает приемлемым присваивать корпоративную информацию, поскольку их компании не строго относятся к соблюдению собственных правил.



Требования закона. КТ

Статья 10. Меры по охране конфиденциальности информации должны включать в себя … **ограничение доступа** к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и **контроля за соблюдением такого порядка.**

Стандартные меры защиты ИКТ

Запрет создания ИКТ на неучтенных носителях.

Запрет копирования документа или его части на неучтенные носители.

Контроль печати документов, содержащих ИКТ.

Запрет пересылки ИКТ по незащищенным каналам связи, в том числе – по открытой электронной почте.

Как контролировать соблюдение этих требований?

А если этого не делать?

13 апреля 2011 года Октябрьским районным судом г. Ижевска принято решение о восстановлении на работе, взыскании заработка за время вынужденного прогула и компенсации морального вреда Ф.С.А., ранее уволенного из ОАО «Удмуртнефть» на основании пп.«в» п.6 ч.1 ст.81 ТК РФ за однократное грубое нарушение трудовых обязанностей – разглашение коммерческой тайны, ставшей известной в связи с исполнением трудовых обязанностей.

Основание для принятого решения – выполнение работодателем требований о мерах по установлению режима коммерческой тайны не в полном объем, в том числе - **отсутствие учета лиц**, допущенных к ИКТ.

Требования закона. ПДн

Статья 18[1]. Осуществление **внутреннего контроля** и (или) аудита соответствия обработки персональных данных настоящему Федеральному закону и принятым в соответствии с ним нормативным правовым актам, **требованиям к защите персональных данных**, политике оператора в отношении обработки персональных данных, локальным актам оператора.

Требования закона. ПДн

Статья 19. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие **для защиты персональных данных от неправомерного или случайного доступа** к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Требования закона. ПДн

Статья 19. Обеспечение безопасности персональных данных достигается, в частности:

9) **контролем за принимаемыми мерами** по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

Требования закона. Инсайд

Статья 11. Обеспечение безопасности персональных данных достигается, в частности:

Юридические лица, органы и организации, указанные в законе, Банк России обязаны:

1) разработать и утвердить **порядок доступа к инсайдерской информации**, **правила** охраны ее конфиденциальности и **контроля за соблюдением требований** настоящего Федерального закона и принятых в соответствии с ним нормативных правовых актов;

Разрешительная система доступа

Документально зафиксированная процедура, регламентирующая:

- порядок предоставления доступа к ресурсам
- порядок прекращения прав доступа
- организацию контроля за соблюдением процедуры
- регламент расследования инцидентов, связанных с предоставлением доступа

Порядок предоставления доступа

Регламентирует:

- основания предоставления доступа
- виды предоставляемых пользователям прав и порядок их назначения
- [возможные] ограничения:
  - ✓ периодов времени, когда представляется доступ
  - ✓ местонахождения пользователя, получающего доступ
  - ✓ устройств, с которых предоставляется доступ

Цель разрешительной системы

Оптимальное распределение производственной, коммерческой и финансовой и иной информации между конкретными исполнителями соответствующих работ и документов:

- обеспечивающее предоставление конкретному работнику необходимых сведений для качественного и своевременного выполнения порученных ему работ и возможность их использования
- исключающее возможность ознакомления исполнителя с излишними, не нужными ему для работы, сведениями, предотвращающее неправомерные действия

Основания для доступа

- Письменные (в системе ЭДО) резолюции руководителя или уполномоченных им лиц
- Распорядительные документы предприятия (организации)
- Должностные инструкции работников
- Заявки на доступ к ресурсам

Роли в разрешительной системе

Роль	Полномочия
Пользователь	Имеет доступ к ресурсам и информации на них для выполнения служебных (трудовых) обязанностей
Линейный руководитель	Руководитель структурного подразделения, где работает пользователь, инициирующий заявку на доступ с указанием требуемых прав
Ответственный за ресурс	Лицо, в чьих интересах создан ресурс, согласовывающий заявку на пользователя
Принимающий решение	Лицо, утверждающие заявку и разрешающее конфликты между Линейным руководителем и Ответственным за ресурс
Администратор	Администратор ИС (приложения, сети), выполняющий технические действия по предоставлению Пользователю доступа к ресурсу в соответствии с заявкой
Администратор безопасности	Работник СИБ, контролирующий соблюдение процедуры предоставления доступа и фактические списки пользователей ресурсов (без доступа к данным)

Результат реализации

На каждый конкретный момент времени можно установить:

- какие пользователи и с каким правами имеют доступ к каждому ресурсу
- к каким конкретно ресурсам и с какими правами имеет доступ конкретный пользователь
- каким пользователям, когда и кем был предоставлен доступ с нарушением установленной процедуры

Поддержание статус-кво

- постоянный контроль за соблюдением процедуры
- анализ обоснованности предоставления прав доступа
- выявление инцидентов и их разбирательство
- мониторинг действий пользователей и соблюдения установленных правил

Проблемы мониторинга

Этические

Психологические

Технические

Правовые

Этические проблемы

- Допустимость контроля за действиями работника
- Проявление потенциального недоверия
- Пределы вмешательства
- Возможный доступ к частной жизни
- Возможность злоупотреблений
- Несоответствие заявленных целей контроля фактическим

Психологические проблемы

Первичная психологическая реакция любого индивидуума на контрольные процедуры, которые затрагивают его жизнедеятельность, - это сопротивление ограничению его свободы.

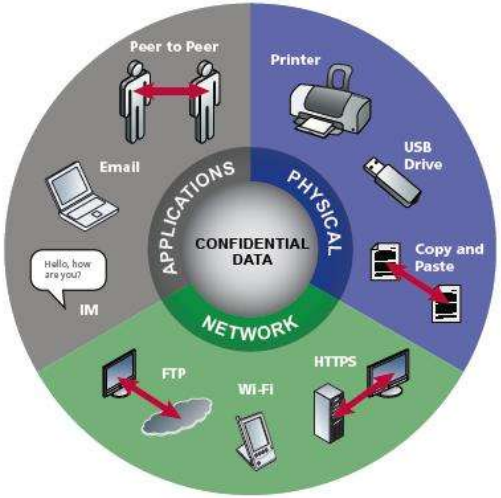
Ханиф Муллахметов,
«Контроль как этическая проблема»

Требования к контролю:

- честность (порядочность)
- объективность
- профессиональная компетентность
- добросовестность
- конфиденциальность

Технические проблемы

- Что и где контролировать
- Какими средствами контролировать
- Кокой функционал необходим для средств контроля
- Как организовать обработку событий безопасности
- Какова допустимая степень автоматизации мониторинга



Правовые проблемы

Статья 23.

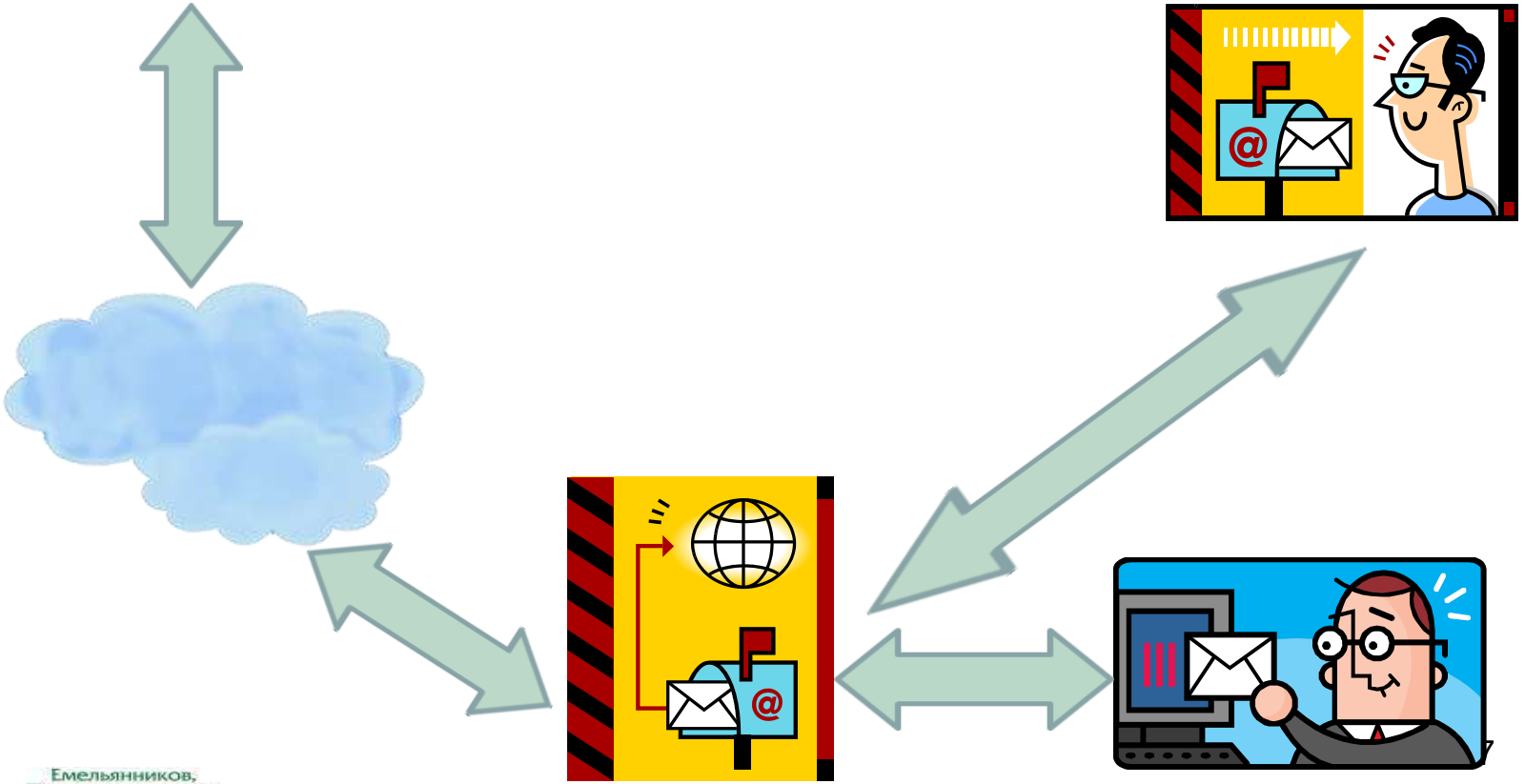
1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.
2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.

Частная жизнь

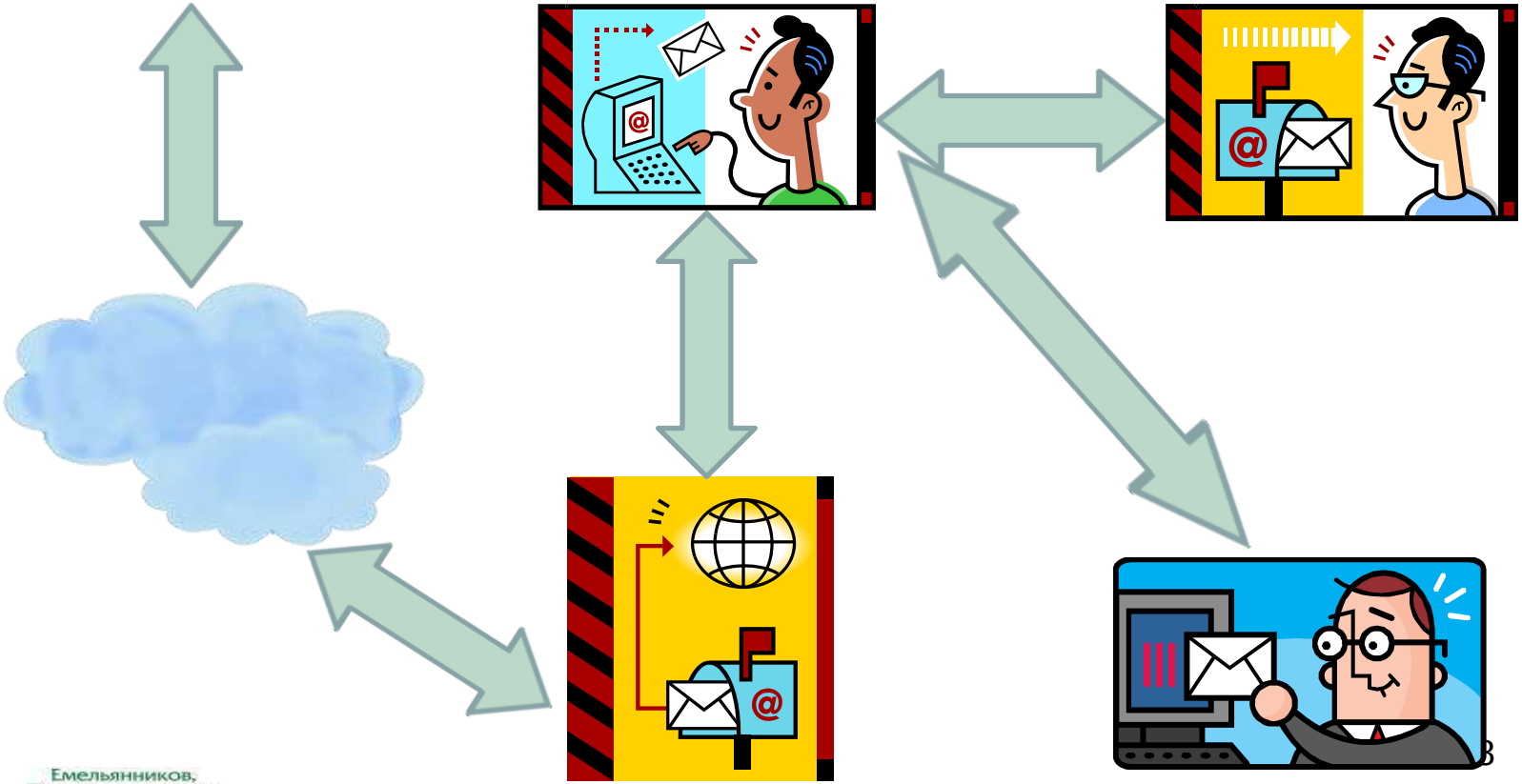
На рабочем месте:

- Компьютер и телефон – для выполнения должностных обязанностей, а не для личных целей.
- Владелец электронного почтового ящика, абонент телефонной сети – организация, а не физическое лицо.
- Работник ведет не личную переписку, а выполняет трудовые обязанности и указания работодателя.
- Весь бумажный документооборот ведется через канцелярию, фактически с перлюстрацией.

Электронная почта?



Изменим маршрутизацию!



Частная жизнь?

Статья 1295. Служебное произведение

2. Исключительное право на служебное произведение принадлежит работодателю, если трудовым или иным договором между работодателем и автором не предусмотрено иное.

Статья 1470. Служебный секрет производства

1. Исключительное право на секрет производства, созданный работником в связи с выполнением своих трудовых обязанностей или конкретного задания работодателя (служебный секрет производства), принадлежит работодателю.

Но права надо закрепить!

Судебная коллегия по гражданским делам Московского городского суда оставила без удовлетворения кассационную жалобу ООО «Айрон Маунтен СНГ» на решение Головинского районного суда г. Москвы **от 17.03.2011.**

Суд отказался признать действия бывшего работника истца по разглашению конфиденциальной информации незаконными и оставил без удовлетворения иск об обязании прекратить разглашение конфиденциальной информации и возместить причиненные убытки.

Истцом не представлено доказательств выполнения при оформлении трудовых отношений положений ст.11 ФЗ «О коммерческой тайне», а именно, что работник был под роспись ознакомлен с перечнем ИКТ, обладателями которой являются работодатель и его контрагенты, и имеющей гриф «коммерческая тайна».

Без чего не обойтись

Прежде, чем организовать мониторинг:

- определить и довести до работников правила использования средств хранения, обработки и передачи информации
- разработать и довести до работников регламент проведения мониторинга
- получить согласие работников на проведение мониторинга использования им средств хранения, обработки и передачи информации
- [опционно] включить положения об обязательстве работника соблюдать правила использования средств коммуникации и согласие на мониторинг в трудовой договор (дополнительное соглашение к трудовому договору)

Что в правилах?

- Указание на то, что средства хранения, обработки и передачи информации принадлежат работодателю, а работник не может рассчитывать на конфиденциальность
- Требование об использовании телефона, факса, электронной почты, доступа в Интернет только для выполнения служебных задач
- Предупреждение о наличии установленного регламента использования электронной почты и доступа в интернет
- Допустимость использования работниками личных устройств для доступа в сеть и порядок их использования
- Запрет на рассылку по незащищенным каналам информации ограниченного доступа
- Ответственноть работника за действия под его аккаунтом

Чего делать не стоит?

- Прослушивать телефонные переговоры, если нет автоматического предупреждения об этом всех абонентов и обоснования прослушивания (улучшение качества обслуживания)
- Контролировать содержание входящих сообщений, направленных в личные почтовые ящики работников
- Использовать результаты контроля любым способом, отличным от указанного в регламенте

Спасибо!
Вопросы?

Емельянников
Михаил Юрьевич
Управляющий партнер
+7 (495) 761 5865
me@mezp.ru
www.emeliyannikov.blogspot.com