

## Контроль управления доступом к конфиденциальной информации и персональным данным

Система контроля управления доступом КУБ позволит обеспечить соответствие информационной системы требованиям нормативных документов (законодательство, а также отраслевые и корпоративные стандарты) по учету и контролю доступа к конфиденциальной информации и к персональным данным в том числе.

### Требования по контролю доступа

В современном законодательстве определены требования к защите конфиденциальной информации, например информации, составляющей коммерческую тайну или содержащей персональные данные. Помимо прочего законодательством определены требования к управлению доступом к конфиденциальной информации и персональным данным:

- **Федеральный закон «О коммерческой тайне»**  
Статья 10 определяет меры по охране конфиденциальности информации и определяет необходимость ограничения доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за его соблюдением. Среди прочего в статье определяется необходимость учета лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана
- **Постановление правительства Российской Федерации N 781 от 17 ноября 2007г. об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных**  
Определяет необходимость учета лиц, получающих доступ к ИСПДн, и формирования соответствующего списка лиц, имеющих права доступа.

Кроме того, во многих отраслевых стандартах и корпоративных инструкциях по информационной безопасности указаны требования по учету и контролю управления доступом к конфиденциальной информации, составляющей коммерческую тайну или включающую персональные данные.

### О чем идет речь?

Если отойти от терминов законодательства, то проблему можно сформулировать следующим образом: эффективная защита конфиденциальной информации подразумевает, помимо прочего, организацию контролируемого процесса предоставления и учета прав доступа к этой информации. Иначе говоря, вы должны в любой момент времени знать и иметь возможность документально подтвердить:

1. Какая информация в организации имеет статус конфиденциальной;
2. Кто из сотрудников или других лиц имеет к ней доступ (как формально, так и фактически);
3. На каком основании был предоставлен доступ к этой информации.
4. Соблюдена ли установленная в организации процедура предоставления доступа
5. Кто, когда и как нарушал установленные правила предоставления доступа и необходимых прав.

Чтобы иметь ответ на эти вопросы в организациях как раз и вводятся формальные процедуры предоставления доступа, которые так не любят рядовые сотрудники.

Здесь следует обратить внимание, что процедуры эти вводятся не только для того, чтобы регламентировать получение доступа, но и для того, чтобы иметь возможность в любой момент получить информацию

текущем состоянии дел по этому вопросу и возможность документально обосновать легитимность предоставленного доступа.

### В чем же проблема?

Современные системы управления доступом позволяют эффективно автоматизировать процессы идентификации пользователей и управления правами доступа сотрудников. Но большинство из них не позволяют отслеживать обоснованность предоставления тех или иных прав доступа.

Одно дело – управлять доступом, и другое – документировать факты запросов (заявки) на доступ и отслеживать их исполнение. Две эти задачи обычно относятся к юрисдикции различных подразделений компании. ИТ-отделы в лице администраторов осуществляют управление доступом на основе разработанных политик безопасности и инструкций. Контролируют же исполнение этих инструкций и соответствие им текущего состояния ИС сотрудники службы информационной безопасности, а в организациях с высоким уровнем зрелости в вопросах охраны конфиденциальности – и владельцы бизнес-процессов, в которых используется информация ограниченного доступа.

Чем критичнее в организации вопросы защиты конфиденциально информации и, соответственно, чем жестче они регулируются корпоративными или законодательными актами, тем жестче выдвигаются требования к системам контроля и учета доступа.

Процесс управления правами доступа в таком случае подразумевает организацию отдельного строго регламентированного документооборота, который учитывает заявки сотрудников на доступ к конфиденциальной информации, процессы их согласования и исполнения, а также позволяет получить юридически значимые ответы на три указанных выше вопроса – «кто», «к каким именно данным» и «на каком основании».

Организовать такой документооборот можно тремя способами:

- 1. Бумажный** – с использованием бумажных заявок и журналов.  
При грамотном использовании такой способ действительно позволяет вести строгий учет прав доступа, но не гарантирует от ошибок, не дает никаких возможностей по своевременному их выявлению, сильно тормозит все процессы в организации, а кроме того делает практически невозможным поиск и анализ заявок и актуализацию списка пользователей в связи с текучестью кадров в больших организациях.
- 2. Автоматизированный** – с использованием специальных заявок, передаваемых по электронной почте или через другие системы обмена сообщениями или документооборота.  
Более быстрый и удобный способ, который наиболее часто встречается в организациях. Не гарантирует от ошибок, не дает возможности отследить фактическое положение дел, а часто не дает юридически значимого подтверждения факта запроса или предоставления доступа.
- 3. Автоматический** – с использованием механизмов заявок, встроенных в системы управления доступом или учетными записями.  
Удобный и оперативный способ, который, тем не менее, не гарантирует соответствия текущего состояния дел политике безопасности, не дает удобных инструментов для отслеживания этого соответствия для службы информационной безопасности и руководства организации и, как и в предыдущем случае, не дает юридически-значимого подтверждения факта запроса или предоставления доступа.

## Решение

Описанную проблему позволяет в полной мере решить система контроля управления доступом КУБ, которая позволяет:

- **Автоматизировать процессы обработки заявок на доступ к ресурсам информационной системы (ИС)** Встроенный механизм документооборота позволяет организовать управление доступом на основе заявок с произвольными цепочками согласования. При этом заявки формулируются в понятных пользователям терминах, и лишь после согласования преобразуются в набор конкретных инструкций для администраторов ИС.
- **Контролировать исполнение заявок на доступ к ресурсам ИС** КУБ позволяет регистрировать все изменения в ИС и сопоставлять их с согласованными заявками.
- **Отслеживать несанкционированные изменения настроек безопасности в ИС** КУБ позволяет осуществлять постоянный мониторинг настроек безопасности ИС и выявлять несанкционированные изменения – изменения, которые не соответствуют согласованным заявкам.

Внедрение системы КУБ позволит раз и навсегда решить вопросы учета и контроля доступа к конфиденциальной информации и персональным данным в организации:

### 1. **Какая информация в организации имеет статус конфиденциальной:**

КУБ помогает сформировать актуальную и эффективную политику безопасности, с помощью таких возможностей, как

- a. автоматическая инвентаризация ресурсов, учетных записей пользователей, а также их прав доступа;
- b. автоматизированный экспорт организационно-штатной структуры (ОШС) из системы кадрового учета предприятия;
- c. автоматизированное сопоставление объектов ОШС и объектов ИС.

### 2. **Кто и на каком основании имеет к доступу конфиденциальной информации (как формально, так и фактически):**

Встроенный документооборот, защищенный ЭЦП, и система отчетов позволяет в любой момент определить, кто и на основании какой заявки имеет доступ к том или иному ресурсу, а также выявить и принять меры к устранению фактов несанкционированного предоставления доступа.

- a. кто инициировал запрос на доступ
- b. кто его согласовал
- c. были ли фактически внесены необходимые изменения в ИС и если да, то кем конкретно

## Вывод

Система контроля управления доступом КУБ позволит обеспечить соответствие ИС требованиям нормативных документов (законодательство, а также отраслевые и корпоративные стандарты) по учету и контролю доступа к конфиденциальной информации и персональным данным.