v 2.2

Требования по ИБ к Порталу

**1. Идентификация**

Каждому пользователю и процессу (при наличии) в системе должен присваиваться уникальный идентификатор.

При необходимости **(обсудить)** можно иметь 2 идентификатора:

- системный (инкрементальный, не используется пользователем);

- пользовательский («читаемый» - логин).

Также необходимо предусмотреть возможность идентификации пользователя по сертификату ЭП (для работы с определенными процедурами – обязательно). В этом случае открытый ключ ЭП «закрепляется» за логином.

*?? из-под какого контекста работают другие системы (порталы)?*

Логин выбирается пользователем самостоятельно при регистрации.

Наличие двух одинаковых логинов в системе не допускается.

Предлагается настоятельно рекомендовать пользователям портала иметь отдельный логин для каждого своего сотрудника.

Заведение пользователя в системе должно осуществляться администратором. Соответствующая роль может быть предоставлена компании-клиенту. Подробнее о ролях см. раздел 5.

**2. Аутентификация**

Проверка подлинности субъекта должна осуществляться путем проверки предъявляемого пароля.

Должна быть реализована возможность требования «сложного» пароля. Для этого необходимо контролировать:

- длину (значение по умолчанию – «>=6»);

- алфавит (обязательное использование как минимум одного символа и одной цифры).

Должна быть реализована возможность смены пароля пользователем самостоятельно. При этом необходимо ввести старое и новое (2 раза) значения пароля.

Должна быть реализована возможность смены пароля администратором. При этом при следующем входе пользователя в систему он должен быть оповещен об этом событии, а также в обязательном порядке должен установить новый пароль.

Срок действия пароля должен быть ограничен (значение по умолчанию – 180 дней). По истечению срока действия пароля пользователю должно быть предложено в обязательном порядке его заменить (должно проверяться, что пароль изменен).

Необходимо предусмотреть опции аутентификации пользователя (выбирает пользователь в личном кабинете):

- вход только по логину-паролю;

- вход только сертификату ЭП;

- вход по сертификату ЭП и паролю (усиленная аутентификация).

При выборе аутентификации по сертификату ЭП, помимо идентификации пользователя по ЭП (проверка открытых полей сертификата на соответствие хранящимся в БД и внесенными в нее при регистрации пользователя), необходимо обеспечить его аутентификацию – проверить владение пользователем закрытым ключом ЭП (путем требования подписать случайную контрольную последовательность с последующей проверкой корректности ЭП).

**3. Управление идентификаторами**

Пароль хранится в БД исключительно в виде хэш-значения (с обязательным добавлением «соли»).

Изменение идентификатора (системного и логина) не допускается.

Удаление идентификатора (системного и логина) не допускается.

Должна быть реализована возможность блокировки логина («ручной» - администратором, или автоматической – при угрозе атаки «подбор пароля», см. раздел 4).

Логины, которые более не предполагается использовать, должны быть аннулированы («супер»-блокировка, восстановление возможно только администратором безопасности портала – сотрудником «Фабриканта»).

**4. Авторизация**

При работе в системе при доступе субъекта к любому объекту (данные, сервис) всегда должны проверяться полномочия данного субъекта на доступ к данному объекту.

Должно соблюдаться и обратное: объект должен быть доступен только тому субъекту, у которого есть соответствующие полномочия.

Для этого должна быть реализована дискреционная модель доступа (матрица доступа), определяющая для каждого объекта субъекты, которые имеют к нему доступ, а также соответствующие полномочия (создание, чтение, изменение, удаление, исполнение и т.п.).

Проверка прав пользователя должна осуществляться:

- при формировании интерфейса;

- перед выполнением операций (обработкой действия пользователя скриптом).

Целостность информации и прав пользователя должна проверяться как минимум один раз – при входе в систему – путем проверки ЭП (см. раздел 5).

Должен вестись подсчет числа попыток ошибочного ввода пароля (подряд). При достижении определенного значения за определенный период времени (по умолчанию – 5 раз в течение 10 минут) логин должен быть заблокирован, а администраторам портала на email направляется уведомление о событии.

Разблокирование логина возможно только администратором (автоматическое разблокирование по истечении некоторого периода времени не допускается).

Запрещается параллельная работа под одним логином: вход в систему, если под этим логином сеанс не завершен, невозможен.

При попытке входа второго пользователя:

- выдается сообщение, что такой пользователь уже работает в системе;

- работающему в системе пользователю направляется popup-сообщение и сообщение в почтовый ящик в личном кабинете;

- фиксируется событие безопасности (см. раздел 7).

Необходимо обеспечить срок активности сессии (принудительное прерывание сеанса доступа в информационную систему после установленного времени бездействия пользователя), по умолчанию – 30 мин.

У пользователя должна быть возможность выйти из системы и тем самым завершить сессию.

**5. Ролевая модель управления доступом**

В целях систематизации полномочий пользователей и упрощения предоставления им необходимых полномочий необходимо реализовать ролевую модель управления доступом субъектов к объектам. Для этого базовые («элементарные») полномочия должны быть сгруппированы по типовым наборам, а права пользователю назначаются через такие типовые наборы.

В целях снижения риска несанкционированной модификации информации и прав пользователя необходимо весь блок данных о нем (включая хэш пароля) подписывать ЭП портала.

При формировании ролей должен соблюдаться принцип минимальных полномочий: в роль добавляются только те полномочия, которые необходимы для ее функционирования.

Предлагаемый **набор ролей**:

администратор безопасности портала (просмотр журнала безопасности портала, блокирование и разблокирование любого логина, восстановление любого аннулированного логина, смена пароля любому логину, просмотр любой информации о пользователе за исключением пароля);

администратор пользователей портала (блокирование и разблокирование любого логина, смена пароля любому логину, заведение нового пользователя, редактирование информации о пользователе, изменение роли пользователя, изменение количества одновременных сессий пользователя);

администратор безопасности клиента (только для своей организации: просмотр журнала безопасности, блокирование и разблокирование логина, смена пароля логину, заведение нового пользователя, редактирование информации о пользователе, изменение роли пользователя, изменение количества одновременных сессий пользователя);

оператор торговых процедур (создание и управление процедурой за исключением отдельных критичных действий – **определить!**);

*Варианты:*

*оператор процедуры (создание процедуры, публикация юридически значимых документов и выполнение юридически значимых действий, кроме заключения договора / контракта);*

*младший оператор процедуры (подготовка проектов документов к публикации);*

*старший оператор процедуры (заключения договора / контракта).*

модератор торговых процедур (какие-то права на модификацию отдельных критичных данных по процедуре);

куратор торговых процедур (просмотр любой открытой для организации-клиента информации о процедуре);

супер-модератор торговых процедур (возможность редактирования процедуры вне зависимости от ее состояния, т.е. в т.ч. вопреки алгоритму ее работы: «откат» процедуры, удаление и добавление документов и т.д. **– определить!**) – предоставляется только сотрудникам портала и доступна только с IP-адреса офиса.

«Админка» Оператора

Аккредитации  
Проверка торгов

Допуск новых участников

Корректировка извещений

**6. Информирование пользователей**

В целях создания дружественного интерфейса пользователи должны оповещаться о следующих фактах:

- ошибка доступа к ресурсам системы (с указанием текущей роли пользователя и минимально необходимой ролью);

- дата, время, IP, окружение прошлого успешного входа (при входе);

- дата, время, IP, окружение прошлого неуспешного входа (при входе);

- попытка входа под логином, для которого открыта активная сессия (см. раздел 4).

**7. Регистрация событий безопасности**

В системе должны быть реализованы распознавание, запись, хранение и защита информации о событиях, относящихся к безопасности информации.

**События**, подлежащие регистрации:

*системные:*

* вход в систему;
* выход из системы;
* заведение пользователя;
* блокирование пользователя;
* аннулирование пользователя;
* редактирование пользователя (без изменения роли и кол. сессий);
* изменение количества сессий пользователя;
* изменение роли пользователя;
* изменение прав доступа к объекту; **- обсудить!**
* просмотр журнала безопасности;
* ошибка ввода пароля пользователя;
* смена пароля;
* сброс пароля;
* нарушение целостности данных пользователя;
* …;

*прикладные:*

* объявление процедуры;
* завершение процедуры;
* просмотр данных о процедуре;
* изменение информации о процедуре;
* изменение параметров процедуры;
* публикация документов;
* редактирование документов;
* удаление документов;
* «откат» процедуры;
* …;

**Состав и содержание** информации о событиях:

*системные:*

* ID субъекта;
* логин;
* код (текстовое описание) события;
* признак успешности (успешно / неуспешно);
* причина (истекло время, нет прав, блокировка, вторая сессия и т.д.);
* критичность (информация, предупреждение, тревога);

*Справочно: тревога – блокировка логина из-за многочисленных ошибок ввода пароля, обнаружение нарушения целостности данных о пользователе; предупреждение – вход в систему супер-модератора, попытка второй сессии под активным логином; остальное – информация).*

* дата;
* время;
* IP;
* информация об окружении (браузер);

*прикладные:*

* ID субъекта;
* логин;
* код (текстовое описание) действия;
* признак успешности (успешно / неуспешно);
* причина (истекло время, нет прав и т.д.);
* информация об объекте (наименование файла, значение данных);

В случае невозможности системы записать информацию о событии в журнал безопасности в адрес администратора безопасности портала должно быть незамедлительно направлено письмо **(обсудить возможность установления такого факта)**.

**8. Просмотр событий безопасности**

В системе должна быть реализована возможность просмотра и анализа информации о событиях безопасности.

Должна быть обеспечена фильтрация событий по каждому полю.

Должна быть обеспечена возможность поиска событий по каждому полю, в т.ч. по их совокупности с правилами «и» и «или», а также с указанием периода.

Журнал должен выводиться в табличном виде в окно браузера (по 20-30-50) записей на страницу или сохраняться в формате MS Excel.

**9. Защита событий безопасности**

Доступ к журналам безопасности должен быть только у пользователей с соответствующими ролями и только в пределах своей организации (у администраторов портала – ко всем).

Ни у кого не должно быть возможности редактирования журналов безопасности.

**Обсудить:** запись в журнале можно подписывать ЭП (но это большие накладные расходы).

**10. Реагирование на события безопасности**

Должно осуществляться уведомление (по email) о событиях с уровнем критичности «предупреждение» и «тревога»: администратора безопасности портала – обо всех событиях, администратора безопасности клиента – о событиях, связанных с его организацией.

При обнаружении нарушения целостности данных о пользователе соответствующих логин блокируется.