УТВЕРЖДАЮ
Первый заместитель
Губернатора Белгородской области

_____В.А. Сергачёв

«___» _____ 2015г.

ПРАВИЛА
по обеспечению информационной безопасности на рабочем месте пользователя средств криптографической защиты информации в департаменте внутренней и кадровой политики Белгородской области

Белгород 2015

1. Введение

Настоящие правила разработаны в целях обеспечения информационной безопасности на рабочем месте пользователя средств криптографической защиты информации в департаменте внутренней и кадровой политики Белгородской области (далее – Департамент).

Настоящие правила разработаны на основании:

− Федерального закона от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи»;

− Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

− Приказа ФСБ от 09 февраля 2005 года № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

- «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных 8 Центром ФСБ России 21 февраля 2008 года № 149/6/6-622.

2. Основные понятия

Система − автоматизированная информационная система передачи и приема информации в электронном виде по телекоммуникационным каналам связи в виде юридически значимых электронных документов с использованием средств электронной подписи.

Автоматизированное рабочее место (далее - АРМ) – ПЭВМ, с помощью которой пользователь осуществляет подключение для работы в Системе.

Средство криптографической защиты информации (далее СКЗИ) – шифровальные (криптографические) средства защиты информации конфиденциального характера.

Электронная подпись (далее ЭП) - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

Закрытый ключ ЭП - уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для

создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи;

Открытый ключ ЭП - уникальная последовательность символов, соответствующая закрытому ключу ЭП, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств ЭП подлинности ЭП в электронном документе;

Средства ЭП - аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание ЭП с использованием закрытого ключа ЭП, подтверждение с использованием открытого ключа ЭП подлинности ЭП, создание закрытых и открытых ключей ЭП;

Сертификат ключа проверки (далее – СКП) ЭП - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу СКП ЭП;

Удостоверяющий центр (далее – УЦ) - юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче СКП ЭП, а также иные функции;

Квалифицированный сертификат ключа проверки (далее – КСКП) – СКП ЭП, выданный аккредитованным УЦ или доверенным лицом аккредитованного УЦ либо федеральным органом исполнительной власти, уполномоченным в сфере использования ЭП;

Владелец СКП ЭП - лицо, которому в установленном порядке выдан СКП ЭП;

Подтверждение подлинности ЭП в электронном документе − положительный результат проверки соответствующим средством ЭП принадлежности ЭП в электронном документе владельцу СКП ЭП и отсутствия искажений в подписанном данной ЭП электронном документе.

Компрометация ключа − утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.

3. Общие положения

Условия признания электронных документов, подписанных ЭП, равнозначными документам на бумажном носителе, подписанным собственноручной подписью:

1. Информация в электронной форме, подписанная квалифицированной ЭП, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, кроме случая, если федеральными законами или принимаемыми в соответствии с ними

нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.

2. Информация в электронной форме, подписанная простой ЭП или неквалифицированной ЭП, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия.

3. Если в соответствии с федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или обычаем делового оборота документ должен быть заверен печатью, электронный документ, подписанный усиленной ЭП и признаваемый равнозначным документу на бумажном носителе, подписанному собственноручной подписью, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью и заверенному печатью.

4. Одной ЭП могут быть подписаны несколько связанных между собой электронных документов (пакет электронных документов). При подписании ЭП пакета электронных документов каждый из электронных документов, входящих в этот пакет, считается подписанным ЭП того вида, которой подписан пакет электронных документов.

4. Риски использования ЭП

При использовании ЭП существуют определенные риски, основными из которых являются следующие:

1. Риски, связанные с отрекаемостью (отказом от содержимого документа). Лицо, на которое указывает подпись под документом, может заявить о том, что документ был изменен и не соответствует документу, подписанному данным лицом.

2. Риски, связанные с несанкционированным доступом (использованием ЭП без ведома владельца). В случае компрометации ключа ЭП или несанкционированного доступа к средствам ЭП может быть получен документ, порождающий юридически значимые последствия и исходящий от имени пользователя, ключ которого был скомпрометирован.

Для снижения данных рисков или их избежание помимо определения порядка использования электронной подписи при электронном взаимодействии предусмотрен комплекс правовых и организационно-технических мер обеспечения информационной безопасности.

5. Порядок действий пользователя

На АРМ пользователя Системы используется СКЗИ для обеспечения целостности, авторства и конфиденциальности информации, передаваемой в рамках информационной системы.

Порядок обеспечения информационной безопасности при работе в Системе определяется организацией, подключающейся к Системе, на основании действующего российского законодательства в области защиты информации.

Владелец СКП обязан:

• Не использовать для ЭП и шифрования открытые и закрытые ключи, если ему известно, что эти ключи используются или использовались ранее.

• Хранить в тайне закрытый ключ.

• Незамедлительно сообщить в УЦ об утрате СКП при наличии оснований полагать, что тайна закрытого ключа нарушена (компрометация ключа).

• Сообщить администратору безопасности об инциденте.

• Обновлять сертификат ключа ЭП в соответствии с установленным регламентом.

Установку и настройку СКЗИ на АРМ Системы производит организация, имеющая лицензию ФСБ РФ на распространение шифровальных (криптографических) средств, разрешенных установленным порядком к применению на территории Российской Федерации. Перед установкой необходимо проверить целостность программного обеспечения СКЗИ. Запрещается устанавливать СКЗИ, целостность которого нарушена.

6. Порядок обращения с СКЗИ в Департаменте

В Департаменте должен быть определен и утвержден порядок учета, хранения и использования носителей ключевой информации с закрытыми ключами ЭП и шифрования, который должен полностью исключать возможность несанкционированного доступа к ним.

Должен быть определен и утвержден журнал учета СКЗИ, поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов.

Должен быть утвержден список лиц, имеющих доступ к ключевой информации.

Для хранения носителей закрытых ключей ЭП и шифрования в помещениях должны устанавливаться надежные металлические хранилища (сейфы), оборудованные замками, обеспечивающими надежное запирание.

В случае увольнения или перевода в другое подразделение (на другую должность), изменения функциональных обязанностей сотрудника, имевшего доступ к ключевым носителям (ЭП и шифрования), должна быть проведена

смена ключей, к которым он имел доступ (защищенный носитель подлежит сдаче администратору безопасности).

ЭП, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие ЭП необходимо немедленно вывести из действия.

Пользователи криптосредств обязаны:

- не разглашать информацию о ключевых документах;
- не допускать снятие копий с ключевых документов;
- не допускать вывод ключевых документов на дисплей (монитор) ПЭВМ или принтер;
- не допускать записи на ключевой носитель посторонней информации;
- не допускать установки ключевых документов в другие ПЭВМ.

7. Учет СКЗИ, поэкземплярного учет криптосредств, эксплуатационной и технической документации к ним, ключевых документов

Используемые или хранимые криптосредства, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету с занесением соответствующих записей в журнал поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов. В журнале должны отражаться следующие записи:

• наименование СКЗИ:
• регистрационный номер СКЗИ;
• номер экземпляров ключевых документов;
• отметка о получении;
• отметка о выдаче;
• отметка о подключении (установке) СКЗИ;
• отметка об изъятии СКЗИ из аппаратных средств информационной системы персональных данных.

Лист ознакомления с ПРАВИЛАМИ по обеспечению информационной безопасности на АРМ пользователя СКЗИ в департаменте внутренней и кадровой политики Белгородской области от «__» _____2015 года

№ п/п	Ф.И.О.	Дата	Подпись
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			
21.			
22.			
23.			
24.			
25.			
26.			
27.			
28.			
29.			
30.			
31.			
32.			
33.			

34.			
35.			
36.			
37.			
38.			
39.			
40.			
41.			
42.			
43.			
44.			
45.			
46.			
47.			
48.			
49.			
50.			
51.			
52.			
53.			
54.			
55.			
56.			
57.			
58.			
59.			
60.			
61.			
62.			
63.			
64.			
65.			
66.			
67.			
68.			
69.			
70.			
71.			
72.			