ПРАВИТЕЛЬСТВО ПЕНЗЕНСКОЙ ОБЛАСТИ

Р А С П О Р Я Ж Е Н И Е

от 07 июня 2017 года № 261-рП

г.Пенза

Об утверждении Регламента реагирования на компьютерные инциденты, связанные с совершением компьютерных атак, внедрением вредоносного программного обеспечения, а также возможными техническими сбоями в работе и Свода правил по безопасной работе при осуществлении информационного взаимодействия с использованием информационно-телекоммуникационной сети «Интернет»

В целях обеспечения безопасности информации в исполнительных органах государственной власти, а также исполнения распоряжения Правительства Пензенской области от 15.03.2017 № 104-рП «Об утверждении Плана мероприятий по защите информации в Пензенской области на 2017–2019 годы», руководствуясь Законом Пензенской области от 22.12.2005 № 906-ЗПО «О Правительстве Пензенской области» (с последующими изменениями):

1. Утвердить прилагаемые:

1.1. Регламент реагирования на компьютерные инциденты информационной безопасности, связанные с совершением компьютерных атак, внедрением вредоносного программного обеспечения, а также возможными техническими сбоями в работе (далее – Регламент);

1.2. Свод правил по безопасной работе при осуществлении организации информационного взаимодействия с использованием информационно-телекоммуникационной сети «Интернет» (далее – Свод правил).

2. Управлению информационных технологий и связи Пензенской области обеспечить координацию исполнения Регламента и Свода правил.

3. Исполнительным органам государственной власти Пензенской области:

3.1. Осуществлять деятельность в соответствии с Регламентом и Сводом правил.

3.2. Назначить лиц, ответственных за исполнение Регламента и Свода правил.

3.3. Ознакомить сотрудников исполнительных органов государственной власти Пензенской области с Регламентом и Сводом правил.

4. Рекомендовать органам местного самоуправления муниципальных образований Пензенской области использовать в работе Регламент и Свод правил.

5. Контроль за исполнением настоящего распоряжения возложить на заместителя Председателя Правительства Пензенской области, координирующего вопросы информатизации органов государственной власти и муниципальных образований Пензенской области.

Исполняющий обязанности
Губернатора Пензенской области Н.П. Симонов

УТВЕРЖДЕН
распоряжением Правительства
Пензенской области
от 07.06.2017 № 261-рП

Р Е Г Л А М Е Н Т
реагирования на компьютерные инциденты информационной безопасности, связанные с совершением компьютерных атак, внедрением вредоносного программного обеспечения, а также возможными техническими сбоями в работе

1.Термины и определения

Информационная безопасность (далее – ИБ) – это процесс обеспечения конфиденциальности, целостности и доступности информации.

Событие информационной безопасности – идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики ИБ или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.

Инцидент информационной безопасности (далее – инцидент ИБ) − одно или серия нежелательных или неожиданных событий в системе информационной безопасности, которые имеют большой шанс скомпрометировать деловые операции и поставить под угрозу защиту информации.

Специалист по защите информации – ответственное лицо за выполнение функций по технической защите информации в исполнительном органе государственной власти Пензенской области.

Пользователь – сотрудник исполнительного органа государственной власти Пензенской области.

Автоматизированное рабочее место (далее – АРМ) – индивидуальный комплекс технических и программных средств, предназначенный для автоматизации профессионального труда специалиста и обеспечивающий подготовку, редактирование, поиск и выдачу на экран и печать необходимых ему документов и данных.

2. Общие положения

Настоящий Регламент разработан в соответствии с федеральными законами от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных» (с последующими изменениями), от 06.04.2011 № 63-ФЗ «Об электронной подписи» (с последующими изменениями), от 21.07.1993 № 5485-1 «О государственной тайне» (с последующими изменениями).

Целью регламента является обеспечение своевременного реагирования и оповещения об инцидентах информационной безопасности при повседневной работе сотрудников в исполнительных органах государственной власти Пензенской области.

Пользователь и специалист по технической защите информации в своей работе руководствуется Регламентом, а также иными руководящими, нормативными документами и регламентирующими документами в области информационной безопасности.

3. События информационной безопасности, приводящие к возникновению инцидентов информационной безопасности

В качестве событий информационной безопасности, приводящих к инцидентам информационной безопасности, могут быть:

- появление файлов с нетипичным именем, форматом или большим размером;
- исчезновение файлов или папок;
- модификация файлов или их содержимого;
- выполнение процессов, не запускаемых пользователем;
- значительное замедление работы программного обеспечения;
- резкое сокращение свободного пространства на жестком диске;
- блокировка экрана монитора или средств ввода/вывода информации;
- появление рекламных или иных баннеров на экране монитора;
- самопроизвольное скачивание и/или запуск/установка файлов;
- изменение/блокировка учетных данных пользователя или доступа к ресурсам;
- умышленные действия пользователя, включающие самовольную установку системного и/или программного обеспечения, а также действия, приведенные в п.3.5 Свода правил по безопасной работе при осуществлении информационного взаимодействия с использованием информационно-телекоммуникационной сети «Интернет», приводящие к техническим сбоям в работе компьютерного оборудования (отказу в обслуживании);
- другие события, которые могут привести к несанкционированному доступу к ресурсам или отказу в обслуживании.

4. Первоочередные меры при обнаружении инцидента информационной безопасности, связанного с совершением компьютерных атак и внедрением вредоносного программного обеспечения

Инцидентом информационной безопасности, связанного с совершением компьютерных атак и внедрением вредоносного программного обеспечения, необходимо считать состояние системы, которое привело к несанкционированному доступу к служебной информации и/или ресурсам исполнительного органа государственной власти Пензенской области, а также отказу в обслуживании вследствие наступления одного или нескольких состояний информационной безопасности.

При наступлении инцидента информационной безопасности важно не пытаться самостоятельно изменять расширения зараженных файлов, а также удалять любые файлы с рабочего компьютера и электронные сообщения.

Основными первоочередными мерами по нейтрализации последствий инцидентов информационной безопасности, связанных с совершением компьютерных атак и внедрением вредоносного программного обеспечения, являются:

- отключение АРМ сотрудника от локальной сети исполнительного органа власти Пензенской области (производится незамедлительно при обнаружении события информационной безопасности, приводящего к возникновению инцидента информационной безопасности);

- отключение АРМ сотрудника от информационно-телекоммуникационной сети «Интернет» (производится незамедлительно при обнаружении события информационной безопасности, приводящего к возникновению инцидента информационной безопасности);

- незамедлительное оповещение специалиста по защите информации исполнительного органа государственной власти Пензенской области;

- незамедлительное отключение питания компьютера (при отключении питания компьютера не пытаться его перезагрузить или включить заново, так как эти действия приводят к изменению файловой системы);

- подготовка докладной записки на имя руководителя исполнительного органа государственной власти Пензенской области, в которой отразить последовательность действий, приведших к наступлению инцидента информационной безопасности;

- незамедлительное информирование Управления Федеральной службы безопасности Российской Федерации по Пензенской области по телефону 54-13-21 (оперативный дежурный) и головного подразделения (сектора) по технической защите информации Управления информационных технологий и связи Пензенской области по телефону 66-03-46 (66-00-45);

- внесение записи специалистом по защите информации в журнал инцидентов информационной безопасности, приведенный в приложении к настоящему Регламенту.

5. Обязанности должностных лиц при наступлении инцидентов информационной безопасности

5.1. Обязанности пользователя:

5.1.1. Соблюдать требования Свода правил по безопасной работе при осуществлении организации информационного взаимодействия с использованием информационно-телекоммуникационной сети «Интернет» (далее – Свод правил).

5.1.2. Выполнять требования и рекомендации специалиста по технической защите информации в рамках соблюдения политики информационной безопасности исполнительного органа государственной власти.

5.1.3. При обнаружении событий, указанных в п. 3 настоящего Регламента, незамедлительно информировать специалиста по технической защите информации исполнительного органа государственной власти Пензенской области.

5.2. Обязанности специалиста по технической защите информации:

5.2.1. Проводить периодический (первичный и повторный не реже одного раза в год) инструктаж пользователей по вопросу информационной безопасности согласно Своду правил, настоящему Регламенту и действующему законодательству по защите информации. Отметки о проведении инструктажа заносить в журнал регистрации инструктажей и заверять собственноручной подписью инструктируемого участника взаимодействия.

5.2.2. Контролировать соблюдение пользователями Свода правил.

5.2.3. Информировать непосредственное руководство о фактах нарушений требований Свода правил со стороны пользователей.

5.2.4. Обеспечивать функционирование установленных средств защиты информации.

5.2.5. Своевременно информировать руководство об истечении сроков действия сертификатов соответствия на средства защиты информации.

5.2.6. Вести журнал инцидентов информационной безопасности, приведенный в Приложении к настоящему Регламенту.

5.2.7. Представлять по запросу головного подразделения по технической защите информации Пензенской области (Управления информационных технологий и связи Пензенской области) в течение трех рабочих дней отчет об инцидентах информационной безопасности и/или копии журналов инцидентов информационной безопасности.

5.2.8. Обо всех фактах инцидентов, повлекших выход из строя либо временную приостановку автоматизированного рабочего места, информационных ресурсов или серверного оборудования, а также о фактах несанкционированного воздействия, заражения вредоносными программами незамедлительно информировать Управление Федеральной службы безопасности Российской Федерации по Пензенской области по телефону 56-13-21 (оперативный дежурный) и головное подразделение по технической защите информации Управления информационных технологий и связи Пензенской области по телефону 66-03-46 (66-00-45).

При обращении в Управление Федеральной службы безопасности Российской Федерации по Пензенской области или головное подразделение по технической защите информации Управления информационных технологий и связи Пензенской области необходимо указать исполнительный орган государственной власти Пензенской области, уполномоченное лицо исполнительного органа государственной власти Пензенской области, время, дату наступления инцидента информационной безопасности, информацию о событиях, приведших к наступлению инцидента информационной безопасности.

Приложение
к Регламенту реагирования
на компьютерные инциденты,
связанные с совершением
компьютерных атак, внедрением
вредоносного программного
обеспечения, а также возможными
техническими сбоями в работе

ФОРМА ЖУРНАЛА
инцидентов информационной безопасности

№ п/п	Дата и время обнару-жения инцидента ИБ	Кем обнаружен инцидент ИБ (ФИО, должность)	Описание инцидента ИБ	Способ решения инцидента ИБ	Дата и время решения проблемы	Отметка о доведении в УФСБ РФ ПО или УИ ПО (дата, время, кто принял информа-цию)	Подпись системного администратора/ администратора информационной безопасности

УТВЕРЖДЕН
распоряжением Правительства
Пензенской области
от 07.06.2017 № 261-рП

СВОД ПРАВИЛ
по безопасной работе при осуществлении организации информационного взаимодействия с использованием информационно-телекоммуникационной сети «Интернет»

1.Термины и определения

Автоматизированное рабочее место (далее – АРМ) – индивидуальный комплекс технических и программных средств, предназначенный для автоматизации профессионального труда специалиста и обеспечивающий подготовку, редактирование, поиск и выдачу на экран и печать необходимых ему документов и данных.

Пользователь – сотрудник исполнительного органа государственной власти Пензенской области.

Антивирусное программное обеспечение – специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления заражённых (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Резервное копирование – процесс создания копии данных на носителе (жёстком диске, дискете, флэш-накопителе), предназначенном для восстановления данных в оригинальном или новом месте их расположения в случае их повреждения или разрушения.

Вредоносный объект – программное обеспечение, позволяющее получить несанкционированный доступ к вычислительным ресурсам ЭВМ, а также данным, которые на ней хранятся.

Почтовый сервис – компьютерная программа по пересылке и получению электронных сообщений (называемых «письма», «электронные письма» или «сообщения») между пользователями компьютерной сети (в том числе информационно-телекоммуникационной сети «Интернет»).

Ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи.

Электронная подпись – 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.

Специалист по технической защите информации – сотрудник исполнительного органа государственной власти Пензенской области, отвечающий за организацию системы защиты информации.

Уполномоченное лицо – сотрудник исполнительного органа государственной власти Пензенской области, исполняющий функции системного администратора.

Мессенджер – это программа, мобильное приложение или веб-сервис для мгновенного обмена сообщениями.

Иностранные Интернет-сервисы − зарубежные прикладные компьютерные приложения, предоставляющие в информационно-телекоммуникационной сети «Интернет» возможности электронной почты, системы обмена мгновенными сообщениями, голосовой и видеоинформацией, социальных сетей, облачных сервисов.

Аутентификационные данные – информация, используемая для верификации предъявленного идентификатора пользователя.

Компрометация аутентификационных данных – утрата доверия к тому, что используемые аутентификационные данные обеспечивают безопасность информации (утрата, разглашение, кража, взлом).

2. Общие положения

Настоящий Свод правил разработан в соответствии с федеральными законами от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», от 27.07.2004 № 152-ФЗ «О персональных данных» (с последующими изменениями), от 06.04.2011 № 63-ФЗ «Об электронной подписи» (с последующими изменениями), от 21.07.1993 № 5485-1 «О государственной тайне» (с последующими изменениями), приказами Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», совместным приказом Федеральной службы безопасности Российской Федерации и Федеральной службы по техническому и экспортному контролю от 31.08.2010 № 416/№ 489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования» и иными нормативными документами в области информационной безопасности.

Пользователь в своей работе руководствуется Сводом правил, а также иными руководящими, нормативными и регламентирующими документами в области информационной безопасности.

3. Правила безопасности при осуществлении информационного взаимодействия

3.1. Исполнительные органы государственной власти Пензенской области обеспечивают пользователям автоматизированное рабочее место с предустановленным лицензионным системным и прикладным программным обеспечением (на котором обеспечивается своевременная установка обновлений

системы безопасности). Дополнительная установка программ, параметров и компонентов производится только уполномоченным лицом с разрешения специалиста по технической защите информации. При привлечении посторонних лиц для ремонта или настройки автоматизированного рабочего места необходимо присутствие специалиста по технической защите информации.

3.2. Исполнительные органы государственной власти Пензенской области обеспечивают наличие сертифицированных по требованиям безопасности информации межсетевых экранов для каждой точки подключения к информационно-телекоммуникационной сети «Интернет».

3.3. Порядок выполнения регулярного резервного копирования личных файлов и параметров АРМ пользователей в исполнительном органе государственной власти определяется самостоятельно (рекомендуется не реже одного раза в неделю).

3.4. Порядок использования электронной подписи осуществлять в соответствии с Руководством по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи, выданным Удостоверяющим центром Управления Федерального казначейства по Пензенской области, приведенным в Приложении к настоящему Своду правил.

3.5. При эксплуатации АРМ и информационных систем в исполнительных органах государственной власти запрещается:

- использование доступа к информационно-телекоммуникационной сети «Интернет» в личных целях;

- посещение досугово-развлекательных сайтов (игровые сайты, интернет-магазины, сайты «для взрослых», онлайн-кинотеатры);

- распространение и тиражирование информации, служебной информации и информации, за распространение которой предусмотрена уголовная или административная ответственность;

- отключение (блокировка) средств защиты информации;

- подключение к АРМ и локальной вычислительной сети посторонних и личных устройств (смартфонов, телефонов, считывателей информации, излучающих устройств (Wi-Fi, Bluetooth, радиомодемы));

- передача аутентификационных данных посторонним лицам (пароли, логины, ключи электронной подписи). При компрометации аутентификационных данных необходимо сразу сообщить специалисту по технической защите информации;

- использование личной электронной почты на рабочих автоматизированных местах в служебных целях (личным считать почтовый ящик, на который не заключался пользовательский договор с администрацией почтового сервиса, согласованный с Управлением информационных технологий и связи Пензенской области);

- скачивание, открытие файлов и запуск программ, полученных из непроверенных источников;

- использование мессенджеров для обмена служебной информацией, если не заключался пользовательский договор с администрацией сервиса, согласованный с Управлением информационных технологий и связи Пензенской области.

3.6. При эксплуатации АРМ и информационных систем в исполнительных органах государственной власти рекомендуется:

- при выборе пароля для создания и использования учетных записей соблюдать требования парольной политики;

- при вынужденном отсутствии на рабочем месте осуществлять блокировку автоматизированного рабочего места или выход из учетной записи;

- регулярно обновлять антивирусные базы (при возможности настройки антивирусного средства – автоматическое обновление или в ручном режиме – не реже трех дней);

- проводить полную профилактическую проверку автоматизированного рабочего места пользователя антивирусным программным обеспечением на присутствие вредоносных объектов не реже одного раза в квартал. При подозрении на наличие вредоносного программного обеспечения – незамедлительно;

- перед открытием файлов, скачанных из информационно-телекоммуникационной сети «Интернет», осуществлять их проверку антивирусным программным обеспечением на наличие вредоносного кода;

- при получении подозрительного письма на адрес электронной почты от неизвестного адресата проконсультироваться со специалистом по технической защите информации;

- не устанавливать и не использовать в служебных целях иностранные интернет-сервисы.

3.7. При обнаружении событий информационной безопасности, приводящих к инцидентам информационной безопасности, следовать действиям согласно Регламенту реагирования на компьютерные инциденты информационной безопасности, связанные с совершением компьютерных атак, внедрением вредоносного программного обеспечения, а также возможными техническими сбоями в работе.

4. Парольная политика

4.1. При формировании пароля рекомендуется использовать символы трех категорий из числа категорий, приведенных ниже:

- прописные буквы английского алфавита от A до Z;

- строчные буквы английского алфавита от a до z;

- цифры (от 0 до 9);

- символы, не принадлежащие алфавитно-цифровому набору (например: @,!, $, #, %).

4.2. В соответствии с правилами безопасности запрещается:

- использовать пароль, состоящий менее чем из шести символов;
- использовать в качестве пароля имя учетной записи пользователя или какую-либо его часть;
- включать в пароль легко вычисляемые сочетания символов, простые пароли типа «123», «111», «qwerty» и им подобные, а так же ФИО и даты рождения свои и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые могут быть подобраны, основываясь на информации о пользователе;
- использовать в качестве пароля один и тот же повторяющийся символ, либо повторяющуюся комбинацию из нескольких символов (например, «zzzzzz»);
- использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);
- использовать ранее использованные пароли;
- использовать один пароль в разных информационных ресурсах.

5. Правила пользования государственными и муниципальными информационными системами

5.1. АРМ, используемые для работы с государственными и муниципальными информационными системами (далее – ГИС и МИС), должны соответствовать требованиям, изложенным в документации соответствующих ГИС и МИС.

5.2. Перед началом работы в ГИС и МИС пользователи должны ознакомиться с правилами работы в соответствующих ГИС и МИС (инструкциями пользователям).

5.3. Руководителем исполнительного органа государственной власти Пензенской области определяется периодичность контроля защищенности эксплуатируемых информационных систем (не реже одного раза в квартал).

Приложение
к Своду правил по безопасной работе
при осуществлении организации
информационного взаимодействия
с использованием информационно-
телекоммуникационной
сети «Интернет»

Р У К О В О Д С Т В О
по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи

1. Общие положения

Настоящее руководство составлено в соответствии с требованиями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» и является средством официального информирования лиц, заинтересованных в получении или владеющих квалифицированной электронной подписью, об условиях, рисках и порядке использования квалифицированной электронной подписи и средств электронной подписи, а также о мерах, необходимых для обеспечения безопасности при использовании квалифицированной электронной подписи.

Применение квалифицированной электронной подписи в системах юридически значимого электронного документооборота и иных системах сопровождается рисками финансовых убытков и иного рода потерь, связанных с признанием недействительности сделок, совершенных с использованием квалифицированной электронной подписи при несанкционированном получении злоумышленником ключа электронной подписи или несанкционированного использования рабочего места пользователя, на котором осуществляется выработка квалифицированной электронной подписи. В связи с этим необходимо выполнение приведенных ниже организационно-технических и административных мер по обеспечению правильного функционирования средств обработки и передачи информации.

2. Требования по размещению

При размещении средств квалифицированной электронной подписи:

- должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены средства квалифицированной электронной подписи, посторонним лицам, не имеющим допуск к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями во избежание негативных воздействий с их стороны на средства электронной подписи, средства криптографической защиты и передаваемую информацию;

- внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.

3. Требования по установке средств квалифицированной электронной подписи, общесистемного и специального программного обеспечения

При использовании средств квалифицированной электронной подписи должны выполняться следующие меры по защите информации от несанкционированного доступа:

Необходимо разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.), использовать фильтры паролей в соответствии со следующими правилами:

- длина пароля должна быть не менее 6 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $,&,*, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов, даты рождения и т.д.), а также сокращения (USER, ADMIN, root, и т.д.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;
- личный пароль пользователь не имеет права никому сообщать;
- периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 90 календарных дней.

При использовании ключей электронных подписей средства вычислительной техники должны быть сконфигурированы с учетом следующих требований:

- не использовать нестандартные, измененные или отладочные версии операционных систем;
- исключить возможность загрузки и использования операционной системы, отличной от предусмотренной штатной работой;
- исключить возможность удаленного управления, администрирования и модификации операционной системы и ее настроек;
- на средствах вычислительной техники с установленными средствами квалифицированной электронной подписи должна быть установлена только одна операционная система;
- все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т.п.);
- режимы безопасности, реализованные в операционной системе, должны быть настроены на максимальный уровень;
- всем пользователям и группам, зарегистрированным в операционной системе, необходимо назначить минимально возможные для нормальной работы права;

- необходимо предусмотреть меры, максимально ограничивающие доступ к:
- ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части):
- системному реестру;
- файлам и каталогам;
- временным файлам;
- журналам системы;
- файлам подкачки;
- кэшируемой информации (пароли и т.п.);
- отладочной информации.

Кроме того, необходимо организовать стирание (по окончании сеанса работы средств квалифицированной электронной подписи) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе их работы. Если это невыполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям.

Должно быть исключено попадание в систему программ, позволяющих использовать ошибки операционной системы, для повышения предоставленных привилегий.

Необходимо регулярно устанавливать пакеты обновлений безопасности операционной системы (Service Packs, Hot fix и т.п.), обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий.

В случае подключения технических средств с установленными средствами квалифицированной электронной подписи к общедоступным сетям передачи данных необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов, полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети. С целью исключения возможности несанкционированного доступа к системным ресурсам используемых операционных систем к программному обеспечению, в окружении которого функционируют средства квалифицированной электронной подписи, и к компонентам средств квалифицированной электронной подписи со стороны указанных сетей должны использоваться дополнительные методы и средства защиты (например: установка межсетевых экранов, организация VPN-сетей и т.п.). Все средства защиты должны иметь сертификат уполномоченного органа по сертификации средств защиты.

Организовать и использовать систему аудита, организовать регулярный анализ результатов аудита.

Организовать и использовать комплекс мероприятий по антивирусной защите.

Запрещается:

- осуществлять несанкционированное копирование ключевых носителей;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер и иные средства отображения информации;
- использовать ключевые носители в режимах, не предусмотренных штатным режимом использования ключевого носителя;

- вносить какие-либо изменения в программное обеспечение средств квалифицированной электронной подписи;
- работать со средствами квалифицированной электронной подписи при включенных в техническое средство штатных средствах выхода в радиоканал;
- записывать на ключевые носители постороннюю информацию;
- оставлять средства вычислительной техники с установленными средствами квалифицированной электронной подписи без контроля после ввода ключевой информации.

4. Требования по обеспечению информационной безопасности при обращении с носителями ключевой информации, содержащими ключи квалифицированной электронной подписи

4.1. Меры защиты ключей квалифицированной электронной подписи.

Ключи квалифицированной электронной подписи при их создании должны записываться на типы ключевых носителей, которые поддерживаются используемым средством квалифицированной электронной подписи согласно технической и эксплуатационной документации к ним.

Ключи квалифицированной электронной подписи на ключевом носителе могут быть защищены паролем (111111-кодом). При этом пароль (ПИН-код) формирует лицо, выполняющее процедуру генерации ключей, в соответствии с требованиями на используемое средство квалифицированной электронной подписи.

Если процедуру генерации ключей выполняет сотрудник Удостоверяющего центра Федерального казначейства, то он должен сообщить сформированный пароль (ПИН-код) владельцу ключа квалифицированной электронной подписи.

Ответственность за конфиденциальность сохранения пароля (ПИН-кода) возлагается на владельца ключа квалифицированной электронной подписи.

4.2. Обращение с ключевой информацией и ключевыми носителями.

Недопустимо пересылать файлы с ключевой информацией для работы в системах обмена электронными документами по электронной почте сети «Интернет» или по внутренней электронной почте (кроме запросов на сертификат и открытых ключей).

Ключевая информация должна размещаться на сменном носителе информации (floppy-диск, USB-flash накопитель, e-Token, ru-Token и др.). Размещение ключевой информации на локальном или сетевом диске, а также во встроенной памяти технического средства с установленными средствами квалифицированной электронной подписи способствует реализации многочисленных сценариев совершения мошеннических действий злоумышленниками.

Носители ключевой информации должны использоваться только их владельцем либо Уполномоченным лицом на использование данного носителя и храниться в месте, не доступном третьим лицам (сейф, опечатываемый бокс, закрывающийся металлический ящик и т.д.).

Носитель ключевой информации должен быть вставлен в считывающее устройство только на время выполнения средствами квалифицированной электронной подписи операций формирования и проверки квалифицированной электронной подписи, шифрования и дешифрования. Размещение носителя ключевой информации в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключевой информации третьими лицами.

На носителе ключевой информации недопустимо хранить иную информацию (в том числе рабочие или личные файлы).

4.3. Обеспечение безопасности АРМ с установленными средствами квалифицированной электронной подписи.

С целью контроля исходящего и входящего подозрительного трафика технические средства с установленными средствами квалифицированной электронной подписи должны быть защищены от внешнего доступа программными или аппаратными средствами межсетевого экранирования. Эти средства должны пресекать отправку в «Интернет» информации, инициированную программами, не имеющими соответствующих полномочий.

На технических средствах, используемых для работы в системах обмена электронными документами:

- на учетные записи пользователей операционной системы должны быть установлены пароли, удовлетворяющие требованиям, приведенным в разделе 3;
- должно быть установлено только лицензионное программное обеспечение;
- должно быть установлено лицензионное антивирусное программное обеспечение с регулярно обновляемыми антивирусными базами данных;
- должны быть отключены все неиспользуемые службы и процессы операционной системы Windows (в т.ч. службы удаленного администрирования и управления, службы общего доступа к ресурсам сети, системные диски С: и т.д.);
- должны регулярно устанавливаться обновления операционной системы;
- должен быть исключен доступ (физический и/или удаленный) к техническим средствам с установленными средствами квалифицированной электронной подписи и средствами криптографической защиты третьих лиц, не имеющих полномочий для работы в системе обмена электронными документами;
- должна быть активирована подсистема регистрации событий информационной безопасности;
- должна быть включена автоматическая блокировка экрана после ухода ответственного сотрудника с рабочего места.

В качестве автоматизированного рабочего места для работы в системах обмена электронными документами крайне не рекомендуется выбирать переносной компьютер (ноутбук). Если выбран ноутбук, недопустимо его подключение к сетям общего доступа в местах свободного доступа в «Интернет» (интернет-кафе, гостиницы, офисные центры и т.д.), при этом для хранения ключевой информации должен использоваться сменный носитель информации.

В случае передачи (списания, сдачи в ремонт) сторонним лицам технических средств, на которых были установлены средства квалифицированной электронной подписи, необходимо гарантированно удалить всю информацию, использование которой третьими лицами может потенциально нанести вред организации, в том числе средства квалифицированной электронной подписи, журналы работы систем обмена электронными документами и т.д.).

5. Дополнительные требования

Дополнительные требования по обеспечению информационной безопасности при работе в системах обмена электронными документами могут дополнительно устанавливаться правилами систем ЭДО, требованиями по эксплуатации и безопасности средств квалифицированной электронной подписи.