УТВЕРЖДАЮ

Заместитель руководителя

Федерального казначейства

_____/ Гуральников С.Б. /

«13» марта 2015 г.

УТВЕРЖДАЮ

Заместитель руководителя

Федерального казначейства

_____/ Смирнов В.А. /

«13» марта 2015 г.

Государственная интегрированная информационная система управления общественными финансами «Электронный бюджет»

Требования по обеспечению информационной безопасности автоматизированного рабочего места пользователя системы «Электронный бюджет»

(для квалифицированных специалистов по информационной безопасности)

СОГЛАСОВАНО

Начальник Управления режима секретности и безопасности информации

_____/ Бражко В.С./

«13» марта 2015 г.

СОГЛАСОВАНО

Начальник Управления интегрированных информационных систем государственных финансов

_____/ Гвоздева Н.В. /

«13» марта 2015 г.

Москва, 2014

СОДЕРЖАНИЕ

АННОТАЦИЯ

Данный документ содержит перечень требований по обеспечению информационной безопасности автоматизированного рабочего места Пользователя системы «Электронный бюджет».

Документ предназначен для квалифицированных специалистов по информационной безопасности Организации Пользователя системы «Электронный бюджет».

1. СПИСОК ТЕРМИНОВ И СОКРАЩЕНИЙ

В документе используются следующие термины и сокращения:

АО – аппаратное обеспечение;

АРМ – автоматизированное рабочее место пользователя системы «Электронный бюджет»;

ВВК – воздействие вредоносного кода;

ВК – вредоносный код;

ЛВС – локальная вычислительная сеть;

НСД – несанкционированный доступ;

ОС – операционная система;

ПО – программное обеспечение;

ПАК – программного-аппаратный комплекс;

Пользователь – зарегистрированный в системе «Электронный бюджет» сотрудник организации, которому предоставлен доступ к определенным функциям в системе «Электронный бюджет», в соответствии с заявкой на подключение;

Система «Электронный бюджет» – государственная интегрированная информационная система управления общественными финансами «Электронный бюджет»;

СЗИ – средства защиты информации;

СКЗИ – средства криптографической защиты информации, обеспечивающие создание защищенного соединения с порталом системы «Электронный бюджет» и создание квалифицированной электронной подписи.

.

2. РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ БЕЗОПАСНОЙ ЭКСПЛУАТАЦИИ

2.1. Общие положения

Защита ПО и АО от НСД и воздействия вредоносного кода при установке и использовании АРМ пользователя является составной частью общей задачи обеспечения безопасности информации внешних систем по отношению к системе «Электронный бюджет». Наряду с применением СЗИ от НСД и ВВК, необходимо выполнение целого ряда мер, включающего в себя организационно-технические и административные мероприятия, связанные с обеспечением правильности функционирования технических средств обработки и передачи информации, а также установление соответствующих правил для обслуживающего персонала, допущенного к работе с информацией ограниченного доступа.

Состав СЗИ, применяемых на АРМ пользователя, зависит от способа взаимодействия АРМ пользователя с системой «Электронный бюджет».

По способу взаимодействия с системой «Электронный бюджет» АРМ пользователя подразделяется на следующие типы:

Тип 1. АРМ, взаимодействующий с системой «Электронный бюджет» посредством прямого подключения к сети Интернет.

Тип 2. АРМ, взаимодействующий с системой «Электронный бюджет» посредством подключения к сети Интернет через ЛВС организации.

Тип 3. АРМ, взаимодействующий с системой «Электронный бюджет» посредством подключения по выделенным каналам связи через ЛВС организации.

2.2. Организация работ по защите от НСД

Защита информации от НСД должна обеспечиваться на всех технологических этапах обработки информации, в том числе при проведении ремонтных и регламентных работ. Защита информации от НСД должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем или администратором информационной безопасности. В организации, эксплуатирующей АРМ пользователя, должен быть назначен администратор информационной безопасности, на которого возлагаются задачи организации работ по использованию АРМ пользователя,

выработки соответствующих инструкций для пользователей, а также контроль за соблюдением описанных ниже требований.

2.2.1. Требования по размещению технических средств

При размещении технических средств с установленным АРМ пользователя:

- должны быть приняты меры по исключению НСД в помещения, в которых размещены технические средства с установленным АРМ пользователя, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях;
- внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.

2.2.2. Требования по установке общесистемного и специального ПО

К установке общесистемного и специального ПО допускаются лица, изучившие документацию на ПО. При установке ПО на АРМ пользователя необходимо соблюдать следующие требования:

1) на технических средствах, предназначенных для работы с АРМ пользователя, использовать только лицензионное ПО фирм-изготовителей;
2) установку ПО АРМ пользователя необходимо производить только с зарегистрированного, защищенного от записи носителя;
3) на АРМ пользователя не должны устанавливаться средства разработки ПО и отладчики;
4) предусмотреть меры, исключающие возможность несанкционированного не обнаруживаемого изменения аппаратной части технических средств, на которых установлено ПО АРМ пользователя (например, путем опечатывания системного блока и разъемов АРМ пользователя);
5) после завершения процесса установки должны быть выполнены действия, необходимые для осуществления периодического контроля целостности установленного ПО на АРМ пользователя;

6) ПО, устанавливаемое на АРМ пользователя, не должно содержать возможностей, позволяющих:
   - модифицировать содержимое произвольных областей памяти;
   - модифицировать собственный код и код других подпрограмм;
   - модифицировать память, выделенную для других подпрограмм;
   - передавать управление в область собственных данных и данных других подпрограмм;
   - не санкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;
   - повышать предоставленные привилегии;
   - модифицировать настройки ОС;
   - использовать недокументированные фирмой-разработчиком функции ОС.

2.3. Требования по защите от НСД при эксплуатации АРМ пользователя

При организации работ по защите информации от НСД необходимо учитывать следующие требования:

1) 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 8-ми 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 и т. д.), а также общепринятые сокращения (USER, ADMIN, ALEX и т. д.);
   - при смене пароля новое значение должно отличаться от предыдущего не менее, чем в 4-х позициях;
   - личный пароль пользователь не имеет права сообщать никому;

– периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 6-и месяцев. Число неудачных попыток ввода пароля должно быть ограничено числом 10.

Указанная политика обязательна для всех учетных записей, зарегистрированных в ОС;

2) средствами BIOS должна быть исключена возможность работы на АРМ пользователя, если во время его начальной загрузки не проходят встроенные тесты;

3) запрещается:

– оставлять без контроля вычислительные средства, на которых эксплуатируется АРМ пользователя, после ввода ключевой информации либо иной информации ограниченного доступа;

– осуществлять несанкционированное администратором информационной безопасности копирование ключевых носителей;

– разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п. иные средства отображения информации;

– записывать на ключевые носители постороннюю информацию.

4) администратор информационной безопасности должен сконфигурировать ОС, в среде которой планируется использовать АРМ пользователя, и осуществлять периодический контроль сделанных настроек в соответствии со следующими требованиями:

– не использовать нестандартные, измененные или отладочные версии ОС;

– исключить возможность загрузки и использования ОС, отличной от предусмотренной штатной работой;

– исключить возможность удаленного управления, администрирования и модификации ОС и её настроек;

– режимы безопасности, реализованные в ОС, должны быть настроены на максимальный уровень;

– всем пользователям и группам, зарегистрированным в ОС, необходимо назначить минимально возможные для нормальной работы права;

- должно быть исключено попадание в систему программ, позволяющих, пользуясь ошибками ОС, повышать предоставленные привилегии;
- необходимо регулярно устанавливать пакеты обновления безопасности ОС (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 от возможного воздействия на ОС;
- необходимо организовать и использовать систему аудита, организовать регулярный анализ результатов аудита;
- необходимо организовать и использовать комплекс мероприятий антивирусной защиты;
- необходимо исключить одновременную работу ОС с загруженной ключевой информацией нескольких пользователей.

2.4. Средства защиты от НСД

Для работы АРМ пользователя с системой «Электронный бюджет» требуется применять программно-аппаратные СЗИ от НСД не ниже 6 класса защищенности для СВТ, такие как «Secret Net», «Соболь», «Панцирь-С» и т.п.

2.5. Требования по обеспечению защиты от воздействий вредоносного кода

Вредоносный код – любой программный код (компьютерный вирус, троян, сетевой червь), приводящий к нарушению функционирования средств вычислительной техники и/или предназначенный для искажения, модификации, уничтожения, блокирования или несанкционированного копирования информации. ВК способен создавать свои копии, сохраняющие все его свойства и требующие для своего размножения другие программы, каналы связи или машинные носители.

Возможен следующий характер проявлений действий ВК:

- искажение изображения на экране монитора;
- искажение символов, вводимых с клавиатуры;
- блокирование клавиатуры, звуковые эффекты;
- стирание или порча отдельных частей диска или файлов;

- повреждение загрузочных секторов жесткого диска ПЭВМ и серверов;
- остановка загрузки или зависание компьютера, значительное замедление его работы;
- уничтожение или искажение информации о системной конфигурации АРМ пользователя.

ВК может попасть на компьютер со сменного носителя (CD-ROM, USB флеш-накопителей и других носителей, даже если эти носители не содержат файлов), при загрузке файлов из сети, с сообщением, полученным по электронной почте, а также через уязвимости операционных систем просто при наличии сетевого подключения компьютера к локальной вычислительной сети.

При наличии технической возможности, обновление средств защиты и сигнатурных баз производится централизованно, с рабочего места администратора программных средств защиты от воздействий вредоносного кода. При проведении централизованных обновлений используется механизм ведения протокола средств защиты. Обновление сигнатурных баз производится по мере их выпуска.

В целях обеспечения защиты от воздействий вредоносного кода пользователю АРМ запрещается:

- самостоятельно устанавливать программное обеспечение, в том числе командные файлы;
- использовать при работе «зараженный» вредоносным кодом либо с подозрением на «заражение» носитель и/или файл;
- использовать личные носители на АРМ пользователя;
- использовать служебные носители на домашних компьютерах и в неслужебных целях;
- самостоятельно проводить “лечение” носителя и/или файла;
- самостоятельно отключать, удалять и изменять настройки установленных средств защиты.

Пользователь АРМ обязан:

- проводить контроль на отсутствие ВК любых сменных и подключаемых носителей (CD-дисков, DVD-дисков, USB флеш-накопителей и т.п.) и файлов.

Примечание: Ключевые носители средств криптографической защиты информации контролю на отсутствие ВК не подвергаются;

- на компьютерах с отключенным антивирусным монитором

(постоянной защитой) проводить полную проверку на отсутствие ВК еженедельно (в первый день после выходных);

- при появлении сообщений, формируемых средствами защиты информации, об обнаружении вредоносного кода пользователь АРМ должен немедленно прекратить работу и сообщить об этом руководителю и администратору информационной безопасности (или сотруднику, выполняющему эти функции);
- при невозможности запуска средств защиты информации или при ошибках в процессе их выполнения пользователь АРМ должен немедленно прекратить работу и сообщить об этом руководителю и администратору информационной безопасности (или сотруднику, выполняющему эти функции).

Правила и рекомендации пользователю АРМ по защите от воздействий вредоносного кода:

- первичный входной контроль на отсутствие ВК носителей, предназначенных для многоразовой записи информации (перезаписываемых компакт-дисков и DVD-дисков, USB флеш-накопителей и других подобных носителей) проводит пользователь при первом применении носителя на данном компьютере. Последующие контроли носителя производить перед каждым просмотром состава и содержимого файлов;
- в целях исключения автозапуска исполняемых файлов со сменных носителей (CD, DVD, USB флеш-накопителей и т.п.) пользователю рекомендуется при присоединении носителя к компьютеру (вставка CD/DVD в лоток, вставка USB флеш-накопителей в порт USB) удерживать некоторое время (20-30 секунд) нажатой клавишу Shift;
- входной контроль на отсутствие ВК компакт-дисков и DVD-дисков, предназначенных для одноразовой записи информации, проводит получатель (владелец) диска однократно с момента приобретения (получения) диска перед использованием его на компьютерах.

2.6. Средства по обеспечению защиты от воздействий вредоносного кода

Для работы АРМ пользователя с системой «Электронный бюджет» требуется применять программные средства защиты от воздействия вредоносного кода не ниже 5 класса защищенности по типу Г, таких как:

«Kaspersky Endpoint Security для Windows», «Security Studio Endpoint», «OfficeScan» и т.п.

2.7. Средства межсетевого экранирования

2.7.1. АРМ Тип 1

Взаимодействие АРМ Тип 1 с системой «Электронный бюджет» должно быть защищено с помощью с персонального средства межсетевого экранирования не ниже 4 класса защищенности, таких как: «Континент-АП», «Security Studio Endpoint Protection», «ViPNet Client» и т.п.

2.7.2. АРМ Тип 2 и Тип3

Взаимодействие АРМ Тип 2 и Тип 3 с системой «Электронный бюджет», объектами ЛВС организации и ресурсами сети Интернет должно быть защищено с помощью сетевого (в составе ЛВС Организации) или персонального средства межсетевого экранирования не ниже 4 класса защищенности.

Примеры допустимых к использованию по классу защищенности средств межсетевого экранирования:

- в составе ЛВС организации:
  - АПКШ Континент;
  - Check Point Firewall;
  - ViPNet Coordinator и т.п.
- персональные средства:
  - Security Studio Endpoint Protection;
  - Континент-АП;
  - ViPNet Client (4 класс) и т.п.

2.8. Средства обнаружения вторжений

2.8.1. АРМ Тип 1

Взаимодействие АРМ Тип 1 с системой «Электронный бюджет» должно быть защищено с помощью персонального средства обнаружения вторжений не ниже 6 класса защищенности для СВТ.

В качестве средства обнаружения вторжений может быть использовано ПО «Security Studio Endpoint Protection» либо иное средство, сертифицированное по требуемому классу защищенности.

2.8.2. АРМ Тип 2 и Тип3

Взаимодействие АРМ Тип 2 и Тип 3 с системой «Электронный бюджет», объектами ЛВС организации и ресурсами сети Интернет должно быть защищено с помощью сетевого (в составе ЛВС организации) или персонального средства обнаружения вторжений не ниже 5 класса защищенности.

Примеры допустимых к использованию по классу защищенности средств обнаружения вторжений:

- персональные средства или средства в составе ЛВС организации:
  - Континент-ДА;
  - Security Studio Endpoint Protection и т.п.

2.9. Требования по обращению со средствами криптографической защиты информации

Установка, настройка и сопровождение СКЗИ осуществляется администратором информационной безопасности организации в соответствии с требованиями законодательства Российской Федерации и эксплуатационной документации к СКЗИ.

Первичная установка СКЗИ на автоматизированное рабочее место пользователя системы «Электронный бюджет» осуществляется с оформлением соответствующего акта установки согласно требованиям Регламента Удостоверяющего центра Федерального казначейства.

Формуляр на СКЗИ в электронном виде, находящийся в составе документации на СКЗИ, выводится администратором информационной безопасности организации на бумажный носитель и заполняется от руки в части раздела «Сведения о закреплении изделия при эксплуатации». Ответственное хранение формуляра осуществляется администратором информационной безопасности организации.

Запрещается полное или частичное воспроизведение, тиражирование и распространение оптических носителей, содержащих дистрибутивы СКЗИ, а также лицензионных ключей СКЗИ.

В случае прекращения полномочий организации в системе «Электронный бюджет», оптические носители, содержащие дистрибутивы СКЗИ, и лицензионные ключи СКЗИ, а также заполненные установленным порядком формуляры возвращаются организацией в орган Федерального казначейства (по месту получения СКЗИ).

ЛИСТ СОГЛАСОВАНИЯ

Наименование организации, предприятия	Фамилия, имя, отчество	Должность	Подпись	Дата
УШИСТФ	Баркова И.И.	Нач. отдела		
УРСиБИ	Гаврилов М.Б.	ЗНО		
УРСиБИ	Феоктистов Б.И.	Начальник ООИБЦА		
УРиБИ	Кацуев А.Ю.	Начальник отдела		
УХиБО	Медведев А.Б.	ЗНУ		
УИС	Федоров А.В.	Зам. нач. ОЭПиО		
	Башмур А.В.	Нач. отд. ОТД		
	Колесников И.Я.	Нач. отд.		
	Зевунов Ю.С.	Зам. нач. Упр.		
	Павлов С.Г.	Нач. Упр.		

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номер версии документа	Дата изменения (дд.мм.гггг)	Автор изменения (ФИО)	Комментарии к изменениям
1.0	16.01.2015	Пляцидевский А.Н.	Первоначальная версия документа.