УТВЕРЖДЕН

643.18184162.00006-02 90-ЛУ

ПРОГРАММНЫЙ КОМПЛЕКС «ЭЛЕКТРОННЫЙ ЗАМОК «ВИТЯЗЬ»,

ВЕРСИЯ 2.2

Руководство администратора

643.18184162.00006-02 90

Листов 36

Подп. и дата	
Инв. № дубл.	
Взам. инв. №	
Подп. и дата	
Инв. № подл.	

2024

Литера

АННОТАЦИЯ

Настоящий документ содержит сведения, необходимые для организационно-технического администрирования (приемка, установка и первичная настройка) программного комплекса «Электронный замок «ВИТЯЗЬ», версия 2.2 (далее – ПК «ЭЗ «ВИТЯЗЬ» 2.2), который поставляется интегрированным в системное программное обеспечение (ПО) материнской платы компьютера.

Данное руководство предназначено для персонала администрирования и безопасности.

Описание работы с ПК «ЭЗ «ВИТЯЗЬ» 2.2 приведено в документе «Руководство пользователя» 643.18184162.00006-02 91.

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ О ПК «ЭЗ «ВИТЯЗЬ» 2.2

1.1. Наименование и обозначение

Наименование программного изделия – Программный комплекс «Электронный замок «ВИТЯЗЬ» версия 2.2.

Обозначение программного изделия – 643.18184162.00006-02.

Наименование предприятия-изготовителя – АО «Крафтвэй корпорэйшн ПЛС».

Фактический адрес – 249032, Калужская область, г. Обнинск, Киевское ш., д. 64.

1.2. Назначение

ПК «ЭЗ «ВИТЯЗЬ» 2.2 – это средство доверенной загрузки (СДЗ) уровня UEFI BIOS второго класса защиты со встроенным средством антивирусной защиты (САВЗ) типа «Г» второго класса защиты, разработанный согласно заданию по безопасности и руководящих документов ФСТЭК России 643.18184162.00006-02 94 01.

ПК «ЭЗ «ВИТЯЗЬ» 2.2 предустановлен в ПО уровня UEFI BIOS компьютера и предназначено для использования в автоматизированных системах обработки информации, содержащей сведения, составляющие государственную тайну, а также в государственных информационных системах и информационных системах персональных данных всех классов и уровней защищенности.

Основными угрозами, для противостояния которым используется САВЗ типа «Г», являются угрозы, связанные с внедрением в автономные автоматизированные рабочие места вредоносных компьютерных программ (вирусов) с машинных носителей информации.

ПК «ЭЗ «ВИТЯЗЬ» 2.2 работает на уровне UEFI BIOS и осуществляет:

1) блокирование несанкционированной загрузки нештатной операционной системы (ОС);

2) контроль доступа пользователей к процессу загрузки ОС;

3) контроль целостности (КЦ) ПО и среды функционирования ПК «ЭЗ «ВИТЯЗЬ» 2.2.

ПК «ЭЗ «ВИТЯЗЬ» 2.2 встраивается в UEFI BIOS, что обеспечивает невозможность подключения нарушителя в разрыв между UEFI BIOS и ПК «ЭЗ «ВИТЯЗЬ» 2.2 путем реализации следующих процессов:

1) получение ПК «ЭЗ «ВИТЯЗЬ» 2.2 управления в процессе выполнения кода UEFI BIOS до передачи управления для загрузки ОС с машинного носителя информации;

2) самотестирование ПК «ЭЗ «ВИТЯЗЬ» 2.2;

3) аутентификация пользователя с использованием аутентифицирующих носителей (АН), таких, как USB-ключи и смарт-карты;

4) КЦ среды функционирования (программной среды и компонентов аппаратного обеспечения) ПК «ЭЗ «ВИТЯЗЬ» 2.2;

5) продолжение выполнения кода UEFI BIOS с последующей загрузкой ОС в случае положительной аутентификации пользователя;

6) блокировка загрузки ОС в случае превышения заданного количества неудачных попыток аутентификации пользователя или попытки загрузки нештатной ОС;

7) регистрация событий безопасности и запись информации аудита в выделенную область памяти.

ПК «ЭЗ «ВИТЯЗЬ» 2.2 предназначен для обеспечения нейтрализации следующих основных угроз безопасности информации:

1) для компьютера – это:

– несанкционированный доступ к информации за счет загрузки нештатной ОС и обхода правил разграничения доступа штатной ОС и (или) других средств защиты информации, работающих в среде штатной ОС;

– несанкционированную загрузку штатной ОС и получение несанкционированного доступа к информации;

– нарушение целостности программной среды и (или) состава компонентов аппаратного обеспечения компьютера.

2) для СДЗ – это:

– нарушение целостности ПО;

– отключение и (или) обход нарушителями компонентов ПК «ЭЗ «ВИТЯЗЬ» 2.2;

– несанкционированное изменение конфигурации (параметров);

– преодоление или обход функций безопасности ПК «ЭЗ «ВИТЯЗЬ» 2.2;

– несанкционированное внесение изменений в логику функционирования ПК «ЭЗ «ВИТЯЗЬ» 2.2, в том числе за счет получения остаточной информации, относящейся к ПК «ЭЗ «ВИТЯЗЬ» 2.2 из памяти компьютера и (или) получение доступа к ресурсам, относящимся к ПК «ЭЗ «ВИТЯЗЬ» 2.2 из программной среды компьютера после завершения работы ПК «ЭЗ «ВИТЯЗЬ» 2.2;

– сбои и ошибки в процессе функционирования.

1.3. Условия применения ПК «ЭЗ «ВИТЯЗЬ» 2.2

1.3.1. Требования к аппаратному обеспечению

ПК «ЭЗ «ВИТЯЗЬ» 2.2 поставляется исключительно предустановленным на аппаратную платформу компьютера. Аппаратная платформа, являющаяся средой функционирования ПК «ЭЗ «ВИТЯЗЬ» 2.2, должна быть включена в единый реестр российской радиоэлектронной продукции.

Обязательным параметром аппаратной платформы является наличие микросхемы SPI Flash с объемом свободной памяти не менее 6 Мбайт, которая требуется для работы ПК «ЭЗ «ВИТЯЗЬ» 2.2.

Для хранения настроечной информации и баз данных ПК «ЭЗ «ВИТЯЗЬ» 2.2 может использоваться внешнее сертифицированное энергонезависимое защищенное хранилище. В зависимости от количества объектов, целостность которых будет контролироваться ПК «ЭЗ «ВИТЯЗЬ» 2.2, для хранения списка объектов требуется хранилище размером не менее 325 Кбайт.

Для обеспечения двухфакторной аутентификации ПК «ЭЗ «ВИТЯЗЬ» 2.2 взаимодействует с АН, в качестве которого выступают USB-ключи или смарт-карты. Для обеспечения двухфакторной аутентификации при взаимодействии ПК «ЭЗ «Витязь» с идентифицирующим устройством (ИУ) должны применяться USB-ключи и смарт-карты, сертифицированные по соответствующему конфиденциальности обрабатываемой информации уровню.

Для работы с АН, в качестве которого выступает электронный USB-ключ, требуется один свободный USB-порт. Для работы с АН, в качестве которого выступает смарт-карта, необходим один свободный USB-порт и наличие USB считывателя смарт-карт.

1.3.2. Требования к программному обеспечению

Для функционирования ПК «ЭЗ «ВИТЯЗЬ» 2.2 требуется специализированная UEFI BIOS, которая должна удовлетворять следующим условиям:

1) наличие программного кода, обеспечивающего вызов ПК «ЭЗ «ВИТЯЗЬ» 2.2 до этапа поиска загрузчика ОС;

2) наличие программного кода, пользовательского интерфейса и интерфейсов взаимодействия с ПК «ЭЗ «ВИТЯЗЬ» 2.2 – оболочки Kraftway Secure Shell (KSS), который обеспечивает интерфейс включения/отключения, очистки содержимого хранилища учетных записей пользователей и журналов ПК «ЭЗ «ВИТЯЗЬ» 2.2, получения после аутентификации информации о роли авторизованного пользователя из ПК «ЭЗ «ВИТЯЗЬ» 2.2 с целью обеспечения доступа пользователя с ролью «администратор» к настройкам ПК «ЭЗ «ВИТЯЗЬ» 2.2 и блокирования такого доступа для пользователя с ролью «пользователь».

На компьютер должно быть установлено не более одной штатной ОС.

ПК «ЭЗ «ВИТЯЗЬ» 2.2 может применяться со следующими файловыми системами: FAT16/FAT32, NTFS, ext/ext2/ext3/ext4.

2. ПОРЯДОК ПРИЕМКИ ПК «ЭЗ «ВИТЯЗЬ» 2.2

Учитывая то, что ПК «ЭЗ «ВИТЯЗЬ» 2.2 интегрирован в UEFI BIOS аппаратной платформы и каждый раз при включении компьютера происходит процедура КЦ программных модулей ПК «ЭЗ «ВИТЯЗЬ» 2.2, для приемки ПК «ЭЗ «ВИТЯЗЬ» 2.2 до первого включения компьютера, необходимо:

1) убедиться в том, что аппаратная платформа, на которой установлен ПК «ЭЗ «ВИТЯЗЬ» 2.2 включена в единый реестр российской радиоэлектронной продукции;

2) убедиться в наличии и целостности документа в печатном виде «Программный комплекс «Электронный замок «ВИТЯЗЬ», версия 2.2. Формуляр 643.18184162.00006-02 30», наличии подписей;

3) убедиться в наличии, отсутствии повреждений и читаемости CD с комплектом эксплуатационной документации (ЭД) 643.18184162.00006-02 на ПК «ЭЗ «ВИТЯЗЬ» 2.2.

3. ТРЕБОВАНИЯ ДЛЯ СРЕДЫ ФУНКЦИОНИРОВАНИЯ

Среда функционирования ПК «ЭЗ «ВИТЯЗЬ» 2.2 должна обеспечивать выполнение следующих функций безопасности при эксплуатации ПК «ЭЗ «ВИТЯЗЬ» 2.2:

1) физическая защита компьютера, доступ к которому контролируется ПК «ЭЗ «ВИТЯЗЬ» 2.2;

2) обеспечение доверенного маршрута при взаимодействии с уполномоченными субъектами;

3) обеспечение условий безопасного функционирования ПК «ЭЗ «ВИТЯЗЬ» 2.2;

4) управление атрибутами безопасности компонентов ПК «ЭЗ «ВИТЯЗЬ» 2.2;

5) защита от отключения (обхода).

Для выполнения средой функций безопасности администратор обязан:

1) для реализации физической защиты компьютера обеспечить использование датчика вскрытия корпуса компьютера для контроля доступа к аппаратной платформе, предоставляемого модулем *Контроль целостности оборудования*;

2) для обеспечения доверенного маршрута создать условия безопасной работы пользователей (см. п. 5.1.3) и АН, удовлетворяющие требованиям п. 1.3.1, для строгой двухфакторной аутентификации пользователей ПК «ЭЗ «ВИТЯЗЬ» 2.2 с применением цифровых сертификатов;

3) для реализации условий безопасного функционирования ПК «ЭЗ «ВИТЯЗЬ» 2.2 необходимо обеспечить:

– информирование пользователей о необходимости постоянного соблюдения мер безопасности, изложенных в п. 5.1.1 и п. 5.1.2;

– КЦ системных файлов раздела, содержащего штатную ОС, предоставляемый модулем *Контроль целостности файловой системы* ПК «ЭЗ «ВИТЯЗЬ» 2.2;

– контроль неизменности MBR загрузочного диска и КЦ аппаратного обеспечения, предоставляемый модулем *Контроль целостности оборудования* ПК «ЭЗ «ВИТЯЗЬ» 2.2;

– КЦ программной среды, предоставляемый модулем *Контроль программной среды* ПК «ЭЗ «ВИТЯЗЬ» 2.2;

– регулярную антивирусную проверку среды UEFI, предоставляемую модулем *Антивирус Касперского для UEFI* ПК «ЭЗ «ВИТЯЗЬ» 2.2, а также обновление с определенной периодичностью антивирусных баз;

– надежный источник точного системного времени среды с помощью протокола сетевого времени (NTP) и синхронизацию с определенной периодичностью системного времени

между ПК «ЭЗ «ВИТЯЗЬ» 2.2 и средой для реализации аудита безопасности ПК «ЭЗ «ВИТЯЗЬ» 2.2;

– расширенные возможности по хранению и анализу информации аудита безопасности ПК «ЭЗ «ВИТЯЗЬ» 2.2;

4) для управления атрибутами безопасности обеспечить управление ПК «ЭЗ «ВИТЯЗЬ» 2.2 только уполномоченными администраторами в соответствии с отведенными им ролями;

5) для реализации защиты от отключения (обхода) программных модулей ПК «ЭЗ «ВИТЯЗЬ» 2.2 обеспечить отсутствие в среде функционирования программ для перезаписи микросхемы SPI Flash, содержащей программные модули ПК «ЭЗ «ВИТЯЗЬ» 2.2.

4. НАСТРОЙКА ФУНКЦИЙ БЕЗОПАСНОСТИ СРЕДЫ ФУНКЦИОНИРОВАНИЯ ПК «ЭЗ «ВИТЯЗЬ» 2.2 – ОБОЛОЧКИ KSS И UEFI BIOS

Условные обозначения при описании последовательности действий:

1) названия клавиш клавиатуры приводятся в квадратных скобках, например, [Enter];

2) названия страниц, разделов, пунктов (параметров) оболочки KSS и UEFI BIOS, а также экранных кнопок управления выделяются *курсивом*;

3) значения параметров указываются в кавычках (« »).

4.1. Вход в оболочку KSS

Оболочка KSS, интегрированная в UEFI – это среда защищенного запуска и управления модулями безопасности ПК «ЭЗ «ВИТЯЗЬ» 2.2 до загрузки ОС. Для входа в оболочку имеются следующие варианты действий:

1) вариант 1. При первом запуске компьютера или при выключенном ПК «ЭЗ «ВИТЯЗЬ» 2.2 нужно в процессе загрузки ОС, при появлении окна *Приглашение на вход в KSS* (рис. 1), нажать клавишу [F1] для входа в оболочку KSS, отображается страница *Kraftway Secure Shell* (рис. 2);

Приглашение на вход в KSS

Рис. 1

2) вариант 2. При включенном ПК «ЭЗ «ВИТЯЗЬ» 2.2 нужно пройти процедуру аутентификации для входа в ПК «ЭЗ «ВИТЯЗЬ» 2.2. При появлении окна *Приглашение на вход в*

KSS (см. рис. 1) нажать клавишу [F1] для входа в KSS, отображается страница *Kraftway Secure Shell* (рис. 2).

Страница Kraftway Secure Shell, главное меню оболочки KSS

Рис. 2

Примечание. Если ранее не было выполнено никаких настроек в ПК «ЭЗ «ВИТЯЗЬ» 2.2, то сразу же после отображения Logo-изображения материнской платы (рис. 3) предлагается дождаться начала загрузки ОС или войти в оболочку KSS (см. рис. 1). Все дальнейшие операции, связанные с ПК «ЭЗ «ВИТЯЗЬ» 2.2, сертификатами пользователей и КЦ файловой системы и т.д., доступны только после включения соответствующих модулей безопасности. Набор модулей безопасности определяется спецификацией поставки и может отличаться в различных установках.

Logo-изображение материнской платы

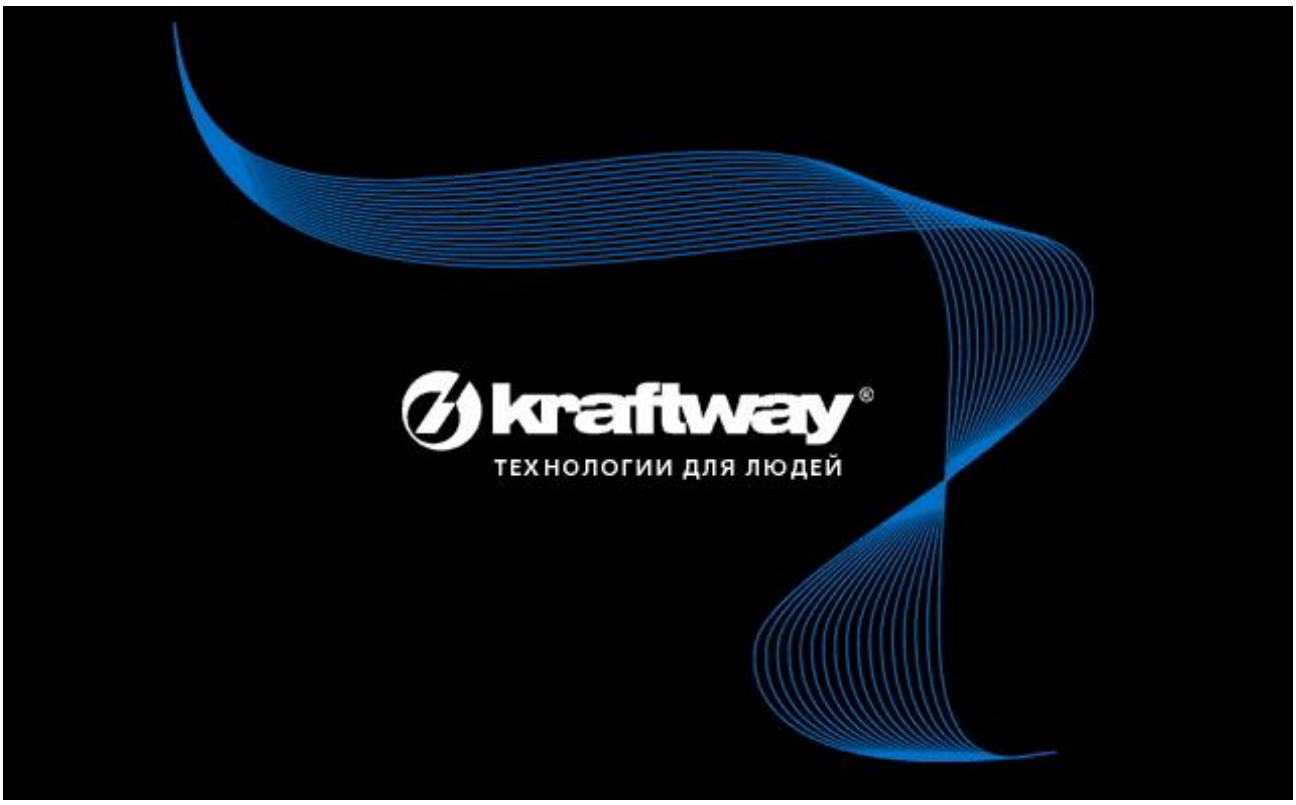


Рис. 3

4.2. Интерфейс пользователя оболочки KSS

Экранная страница оболочки KSS (рис. 4) состоит из следующих областей:

1) область № 1 – для отображения названия экранных страниц оболочки;

2) область № 2 – для отображения:

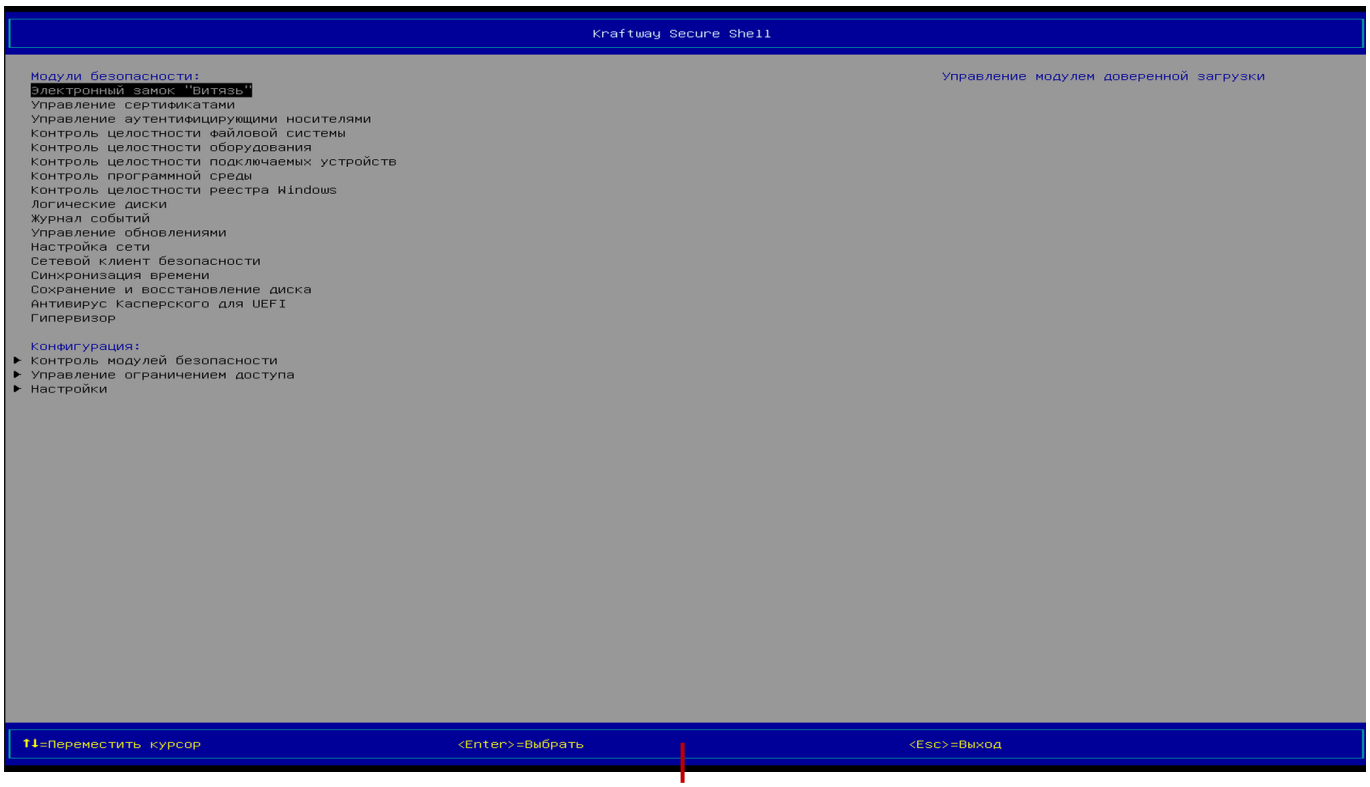
– в левой ее части названия разделов, пунктов, а также значений пунктов меню оболочки;

– в правой ее части дополнительной или справочной информация о пункте (параметре) меню, выбранном в левой части данной области;

– результаты КЦ объектов и отчет о состоянии ПК «ЭЗ «ВИТЯЗЬ» 2.2;

– область № 3 – для отображения информации об используемых на странице клавишах клавиатуры, предназначенных для выполнения определенных действий по навигации в оболочке, выбору пунктов меню, присвоению значений параметрам.

Области оболочки KSS



1 – область для названия пункта/подпункта меню; 2 – область для пунктов/подпунктов меню, дополнительной или справочной информации; 3 – область для подсказок

Рис. 4

Для того чтобы просмотреть данные, которые не уместились в области № 2, следует воспользоваться клавишами [↑], [↓] – для пролистывания данных, для выбора первой строки на странице следует нажать клавишу [Page Up], а для выбора последней строки – клавишу [Page Down].

Главное меню оболочки KSS (см. рис. 4) состоит из двух основных разделов, содержащих следующие пункты:

1) раздел *Модули безопасности*;

– *Электронный замок «Витязь»*;

– *Управление сертификатами;*

– *Контроль целостности файловой системы;*

– *Контроль целостности оборудования;*

– *Контроль программной среды;*

– *Контроль целостности реестра Windows;*

– *Журнал событий;*

– *Антивирус Касперского для UEFI;*

– *Гипервизор;*

2) раздел *Конфигурация*:

– *Контроль модулей безопасности*;

– *Управление ограничением доступа*;

Примечание. Набор модулей безопасности (и соответствующих пунктов меню) определяется спецификацией поставки и может отличаться в различных установках.

4.3. Выход из оболочки KSS

Для выхода из оболочки KSS следует:

1) перейти в главное меню оболочки KSS (см. рис. 2);

2) нажать клавишу [Esc], отображается окно (рис. 5) для подтверждения выхода из оболочки;

Рис. 5

3) нажать клавишу [Enter], предлагается дождаться загрузки ОС.

Примечание. При выходе из оболочки KSS осуществляется очистка оперативной памяти от остаточной информации ПК «ЭЗ «ВИТЯЗЬ» 2.2.

4.4. Настройка параметров оболочки KSS

4.4.1. Время ожидания для входа в оболочку

Для установки времени ожидания (таймаута) для выполнения входа в оболочку перед загрузкой ОС следует:

1) выбрать п. *Настройки* раздела *Конфигурация* главного меню KSS;

2) нажать клавишу [Enter], отображается страница *Настройки* (рис. 6);

Страница *Настройки*

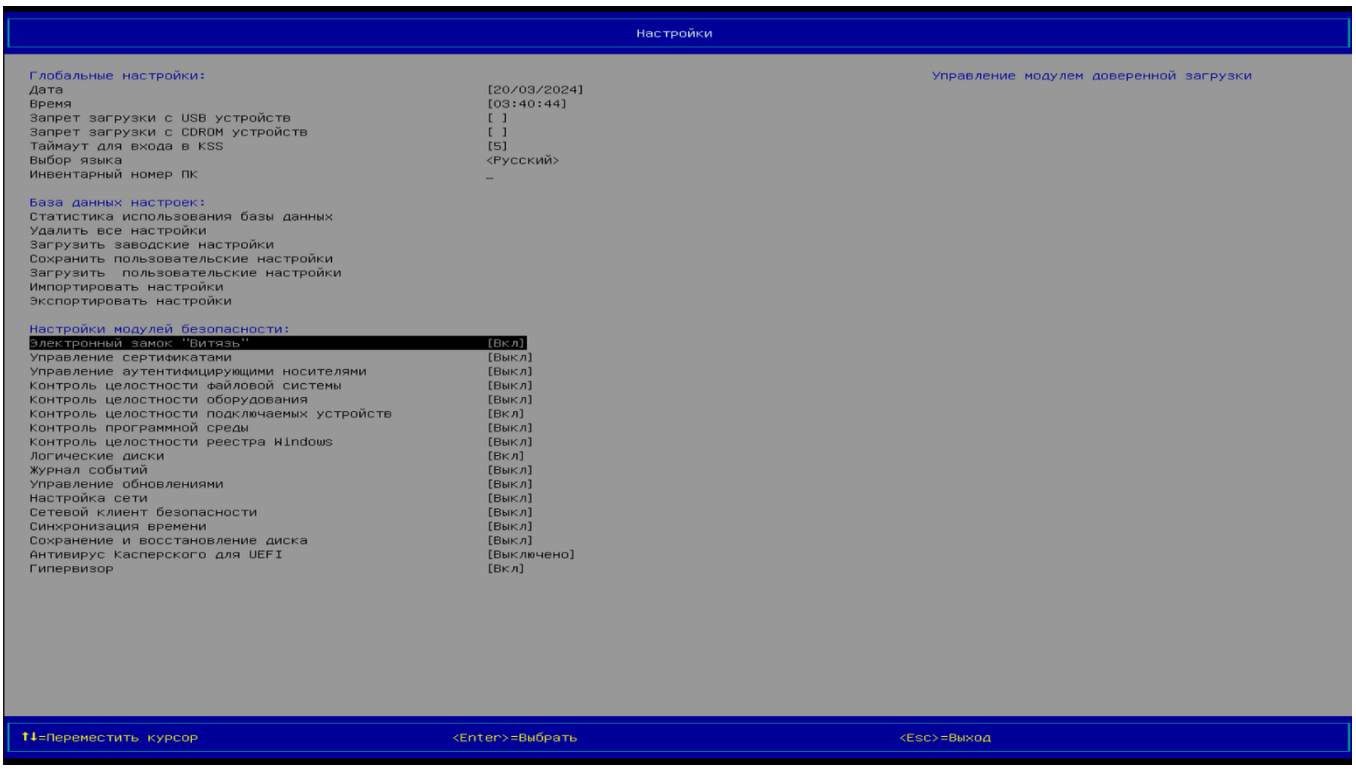


Рис. 6

3) выбрать параметр *Таймаут для входа в KSS* раздела *Глобальные настройки*;

4) установить требуемое значение времени ожидания в секундах клавишами [**+**]/[**-**] цифрового блока клавиатуры (допустимые значения: 1-99).

Примечания:
1. По умолчанию значение параметра *Таймаут для входа в KSS* равно 5;
2. Установить требуемое значение времени ожидания также можно следующим образом:
   – выбрать параметр *Таймаут для входа в KSS* раздела *Глобальные настройки* (см. рис. 6);
   – нажать клавишу [Enter];
   – ввести значение таймаута цифровыми клавишами цифрового блока клавиатуры.

4.4.2. Выбор языка интерфейса

Для выбора языка интерфейса оболочки KSS следует:

1) выбрать п. *Настройки* раздела *Конфигурация* главного меню KSS;

2) нажать клавишу [Enter], отображается страница *Настройки* (см. рис. 6);

3) выбрать п. *Выбор языка* раздела *Глобальные настройки*;

4) нажать клавишу [Enter], отображается окно (рис. 7), предлагающее выбрать язык интерфейса оболочки (доступные значения параметра: «English», «Русский»);

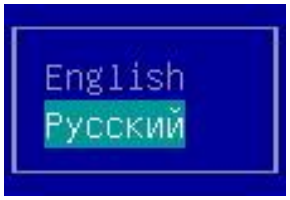


Рис. 7

5) выбрать требуемый язык интерфейса в окне выбора;

6) нажать клавишу [Enter].

4.4.3. Запрет загрузки с USB и CDROM устройств

Для запрета загрузки ОС с USB и CDROM устройств:

1) выбрать п. *Запрет загрузки с USB устройств* раздела *Глобальные настройки*;

2) нажать клавишу [Пробел] и включить запрет;

3) чтобы выключить запрет, нажать клавишу [Пробел] повторно;

4) выбрать п. *Запрет загрузки с CDROM устройств* раздела *Глобальные настройки*;

5) нажать клавишу [Пробел] и включить запрет.

4.4.4. Управление ограничением доступа

Управление *Ограничением доступа* распространяется только на профили пользователей, созданных с ролью *Пользователь*.

Если по конкретному модулю регистрация ограничения доступа запрещена, то наступление события нарушения безопасности этого модуля не ограничит право *Пользователя* на дальнейшие действия в системе.

Для управления регистрацией ограничения доступа следует:

1) выбрать п. *Управление ограничением доступа* раздела *Конфигурация* главного меню KSS;

2) нажать клавишу [Enter], отображается страница *Управление ограничением доступа* (рис. 8);

Страница *Управление ограничением доступа*

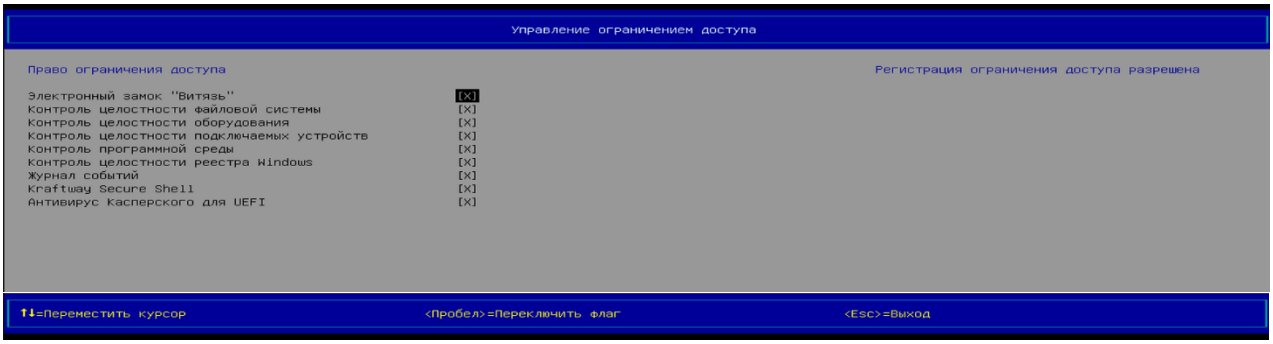


Рис. 8

3) выбрать из раздела *Право ограничения доступа* строку с требуемым модулем;

4) нажать клавишу [Пробел], для переключения флажка состояния регистрации ограничения доступа:

– [X] – регистрация ограничения доступа разрешена;

– [ ] – регистрация ограничения доступа запрещена;

5) нажать клавишу [Esc] для возврата в главное меню.

Примечания:

1. Заданные разрешения/запрещения регистрации ограничения доступа распространяются на все профили пользователей с ролью *Пользователь,* созданные в данном ПК «ЭЗ «ВИТЯЗЬ» 2.2.

2. Модуль, у которого изменяется право ограничения доступа, должен быть включен.

3. При попытке аутентификации *Пользователя* и наступлении события нарушения безопасности модуля, по которому ранее было установлено запрещение регистрации ограничения доступа, система все равно выдаст сообщение о нарушении безопасности. Например, при нарушении целостности оборудования система выдаст сообщение, представленное на рис. 9, но при этом *Пользователь* сможет продолжить свои действия в KSS.

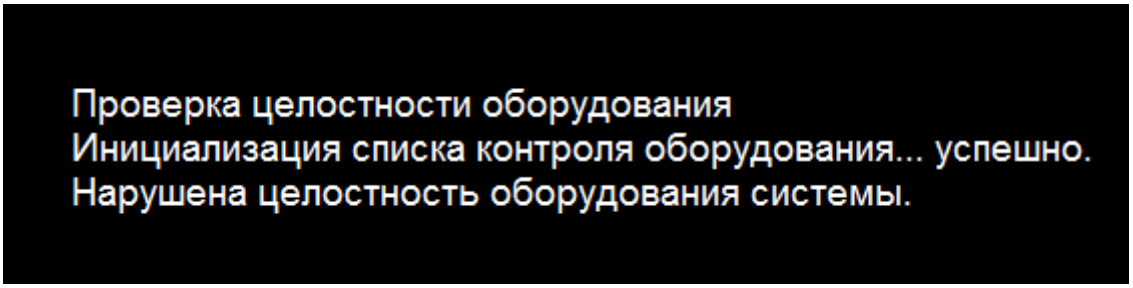


Рис. 9

4.5. Вход в программу настройки UEFI BIOS материнской платы

Пользователи с ролью «администратор», могут входить в программу настройки UEFI BIOS материнской платы (например, для ввода системного времени компьютера).

Для входа в интерфейс настройки UEFI BIOS материнской платы при выключенном ПК «ЭЗ «ВИТЯЗЬ» 2.2 нужно:

1) включить компьютер, на экране отображается Logo-изображение материнской платы (см. рис. 3), а на следующем шаге загрузки отображается приглашение на вход в KSS (см. рис. 1);

2) нажать клавишу [Delete] в момент вывода на экран приглашения на вход в KSS, приглашение на вход в KSS пропадает с экрана;

3) повторно нажать клавишу [Delete], отображается интерфейс UEFI BIOS материнской платы.

Для входа в интерфейс настройки UEFI BIOS материнской платы при включенном ПК «ЭЗ «ВИТЯЗЬ» 2.2 нужно:

1) включить компьютер и пройти процедуру аутентификации для входа в ПК «ЭЗ «ВИТЯЗЬ» 2.2;

2) нажать клавишу [Delete] при выводе на экран приглашения на вход в KSS (см. рис. 1), приглашение на вход в KSS пропадает с экрана;

3) повторно нажать клавишу [Delete], отображается интерфейс UEFI BIOS материнской платы.

5. РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОЙ УСТАНОВКЕ И НАСТРОЙКЕ ПК «ЭЗ «ВИТЯЗЬ» 2.2

5.1. Организационно-технические мероприятия

ПК «ЭЗ «ВИТЯЗЬ» 2.2 готов к использованию по назначению при соблюдении требований по эксплуатации компьютера, в которое оно предустановлено, после размещения компьютера на месте эксплуатации и подключения его к сети электропитания.

Для обеспечения безопасной работы с ПК «ЭЗ «ВИТЯЗЬ» 2.2 допускается его эксплуатация пользователями, изучившими его устройство, правила пользования и меры безопасности, а также прошедшими проверку полученных знаний.

5.1.1. Меры безопасности при использовании ПК «ЭЗ «ВИТЯЗЬ» 2.2

При эксплуатации компьютера с установленным ПК «ЭЗ «ВИТЯЗЬ» 2.2 необходимо выполнять следующие организационно-технические мероприятия по защите информации:

1) правом доступа к компьютеру должны обладать только лица, прошедшие соответствующую подготовку. Администратор безопасности должен ознакомить каждого пользователя, участвующего в эксплуатации ПК «ЭЗ «ВИТЯЗЬ» 2.2, с данными организационно-техническими мероприятиями;

2) должностные инструкции администратора безопасности (его заместителя) и ответственного исполнителя должны учитывать требования данных организационно-технических мероприятий по защите информации;

3) системный блок с установленным ПК «ЭЗ «ВИТЯЗЬ» 2.2 должен быть опечатан специально выделенной для этих целей печатью. Перед каждым включением компьютера необходимо проверять сохранность печатей и разъемов системного блока. Допускается применение дополнительных средств физической защиты системного блока, например, датчика вскрытия корпуса системного блока. После активации такого датчика и соответствующего модуля безопасности ПК «ЭЗ «ВИТЯЗЬ» 2.2, при вскрытии корпуса системного блока пройти далее процедуру аутентификации для входа в ПК «ЭЗ «ВИТЯЗЬ» 2.2 сможет лишь пользователь с ролью «администратор»;

4) в случае обнаружения «посторонних» (не зарегистрированных) программ нарушения целостности, либо выявления факта повреждения печатей на системных блоках работа должна быть прекращена. По данному факту должно быть проведено служебное расследование комиссией в составе представителей служб информационной безопасности организации-владельца сети и организации-абонента сети, где произошло нарушение, и организованы работы по анализу и ликвидации негативных последствий данного нарушения;

5) не допускается оставлять без контроля компьютер с включенным питанием и загруженной ОС. При кратковременном перерыве в работе пользователю рекомендуется

блокировать сеанс и (или) гасить экран, а для возобновления работы предлагать пройти процедуру аутентификации;

6) на компьютер должна быть установлена только одна ОС;

7) должна быть исключена возможность работы на компьютере, если во время его начальной загрузки не проходят встроенные тесты.

5.1.2. Правила безопасной работы пользователя с ролью «администратор» с АН

Администратор обязан соблюдать следующие правила безопасной работы с АН:

1) после получения АН сменить установленный в нем PIN-код для защиты доступа к компьютеру;

2) своевременно менять PIN-код к АН согласно политике безопасности организации;

3) при вводе PIN-кода исключать возможность визуального просмотра его набора другими лицами;

4) не передавать АН, находящийся в распоряжении администратора, другим лицам, а также не оставлять его без присмотра. Попадание АН в чужие руки несет опасность его компрометации;

5) не сообщать PIN-код к АН другим лицам, хранить записанные PIN-коды в недоступном для других лиц месте. Разглашение PIN-кода к АН означает его компрометацию;

6) при утере АН следует немедленно присвоить новый АН учетной записи администратора, АН которой был утерян;

7) беречь АН от механических повреждений;

8) не отсоединять АН от компьютера во время работы с использующими его приложениями. Перед отсоединением АН от компьютера следует завершить работу всех приложений, использующих АН.

5.1.3. Правила безопасной работы пользователя с ролью «пользователь» с АН

Пользователь обязан соблюдать следующие правила безопасной работы с АН:

1) после получения АН сменить установленный в нем PIN-код для защиты доступа к компьютеру;

2) своевременно менять PIN-код к АН согласно политике безопасности организации;

3) при вводе PIN-кода к АН исключать возможность визуального просмотра его набора другими лицами;

4) не передавать АН, находящийся в распоряжении пользователя, другим лицам, а также не оставлять его без присмотра. Попадание АН в чужие руки несет опасность его компрометации;

5) не сообщать PIN-код к АН другим лицам, хранить записанные PIN-коды в недоступном для других лиц месте. Разглашение PIN-кода означает его компрометацию;

6) при утере АН немедленно сообщить об этом администратору;

7) беречь АН от механических повреждений;

8) не отсоединять АН от компьютера во время работы с использующими его приложениями. Перед отсоединением АН от компьютера следует завершить работу всех приложений, использующих АН.

5.2. Установка ПК «ЭЗ «ВИТЯЗЬ» 2.2

ПК «ЭЗ «ВИТЯЗЬ» 2.2 поставляется предустановленным в программную среду компьютера. Дополнительных действий по установке не требуется.

5.3. Активация (включение) ПК «ЭЗ «ВИТЯЗЬ» 2.2

ВНИМАНИЕ! ПК «ЭЗ «ВИТЯЗЬ» 2.2 НАЧНЕТ ВЫПОЛНЯТЬ СВОИ ФУНКЦИИ ТОЛЬКО ПОСЛЕ СОЗДАНИЯ ПРОФИЛЯ ПЕРВОГО АДМИНИСТРАТОРА. РЕКОМЕНДУЕТСЯ СОЗДАТЬ ПРОФИЛЬ ПЕРВОГО АДМИНИСТРАТОРА СРАЗУ ЖЕ ПОСЛЕ ВКЛЮЧЕНИЯ ПК «ЭЗ «ВИТЯЗЬ» 2.2 ДЛЯ ДАЛЬНЕЙШЕЙ РАБОТЫ В НЕМ.

5.3.1. Включение ПК «ЭЗ «ВИТЯЗЬ» 2.2. Метод 1

Для включения ПК «ЭЗ «ВИТЯЗЬ» 2.2 в первый раз или после выключения с очисткой всех данных следует:

1) выбрать п. *Настройки* раздела *Конфигурация* главного меню KSS (см. рис. 2);

2) нажать клавишу [Enter], отображается страница *Настройки* (см. рис. 6);

3) выбрать п. *Электронный замок "Витязь"* раздела *Настройки модулей безопасности*;

4) нажать клавишу [Enter], отображается страница *Электронный замок "Витязь": Настройки* с п. *Включить электронный замок* (рис. 10);

Страница *Электронный замок «Витязь»: Настройки*, п. *Включить электронный замок*

Рис. 10

5) нажать клавишу [Enter], отображается окно (рис. 11), запрашивающее подтверждение на включение ПК «ЭЗ «ВИТЯЗЬ» 2.2;

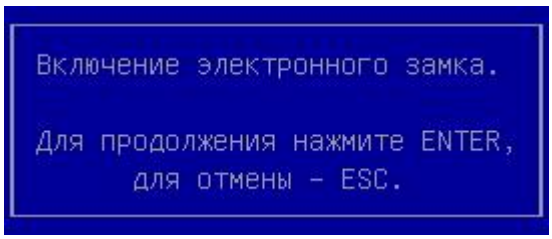


Рис. 11

6) нажать клавишу [Enter], отображается страница *Лицензионное соглашение* (рис. 12);

Страница *Лицензионное соглашение*, п. *Принять лицензионное соглашение*

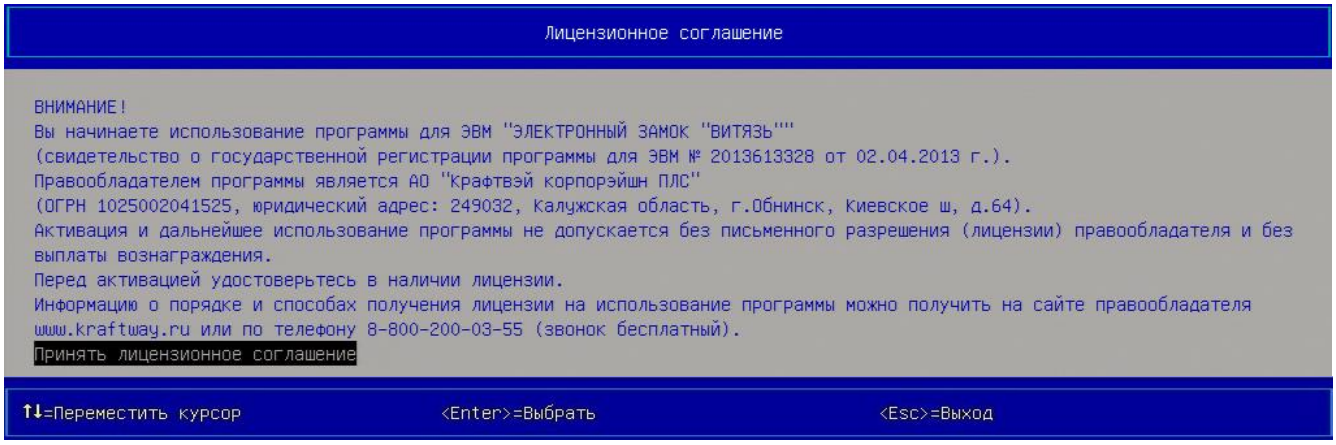


Рис. 12

7) нажать клавишу [Enter], отображается страница *Электронный замок «Витязь»: Настройки* (рис. 13);

Страница *Электронный замок «Витязь» Настройки*, *Способ аутентификации* – «Цифровой сертификат», *Ключевое поле* – «Универсальное имя (UPN)»

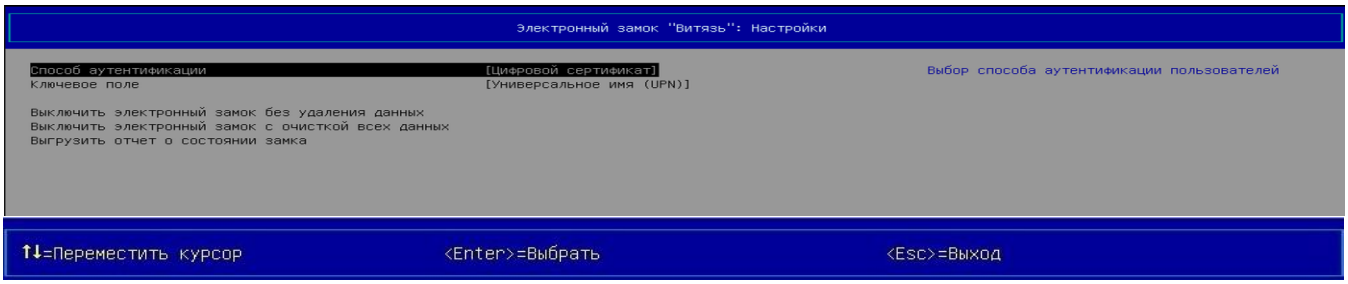


Рис. 13

8) выбрать п. *Способ аутентификации*;

9) нажать клавишу [Enter], отображается окно (рис. 14), предлагающее выбрать способ аутентификации пользователя (доступные значения параметра: «Цифровой сертификат», «Электронный ключ», «Цифровой сертификат и электронный ключ»);

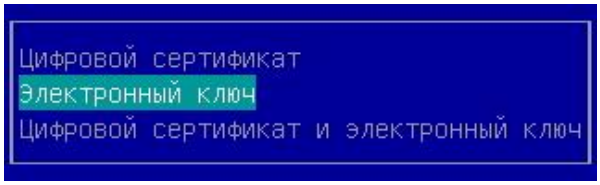


Рис. 14

10) выбрать требуемый способ аутентификации в окне;

11) нажать клавишу [Enter];

12) выбрать п. *Ключевое поле* (см. рис. 13), данный пункт отображается только, если параметру *Способ аутентификации* было присвоено значение «Цифровой сертификат» или «Цифровой сертификат и электронный ключ»;

13) нажать клавишу [Enter], отображается окно (рис. 15), предлагающее выбрать ключевое поле сертификата пользователя, с помощью которого будет выполняться аутентификация пользователя (доступные значения параметра: «Универсальное имя (UPN)», «Общее имя (CN)», «Серийный номер сертификата»);

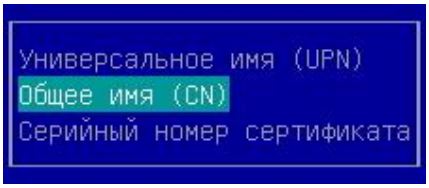


Рис. 15

14) выбрать ключевое поле и нажать клавишу [Enter].

Примечания:

1. При попытке назначения параметрам: *Способ аутентификации*, *Ключевое поле* новых значений, отображается окно (рис. 16), запрашивающее подтверждение на внесение изменений.

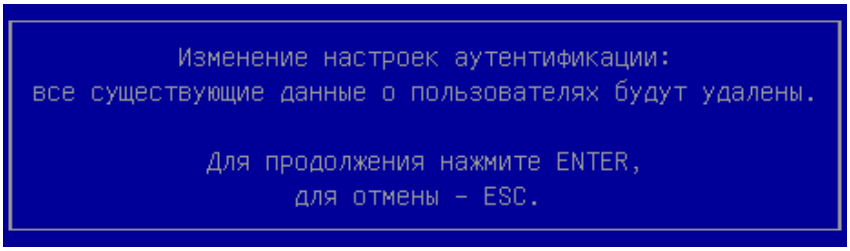


Рис. 16

2. Пункт *Ключевое поле* не выводится на странице *Электронный замок «Витязь» Настройки* (рис. 17), если параметру *Способ аутентификации* было присвоено значение «Электронный ключ».

Страница *Электронный замок «Витязь» Настройки*

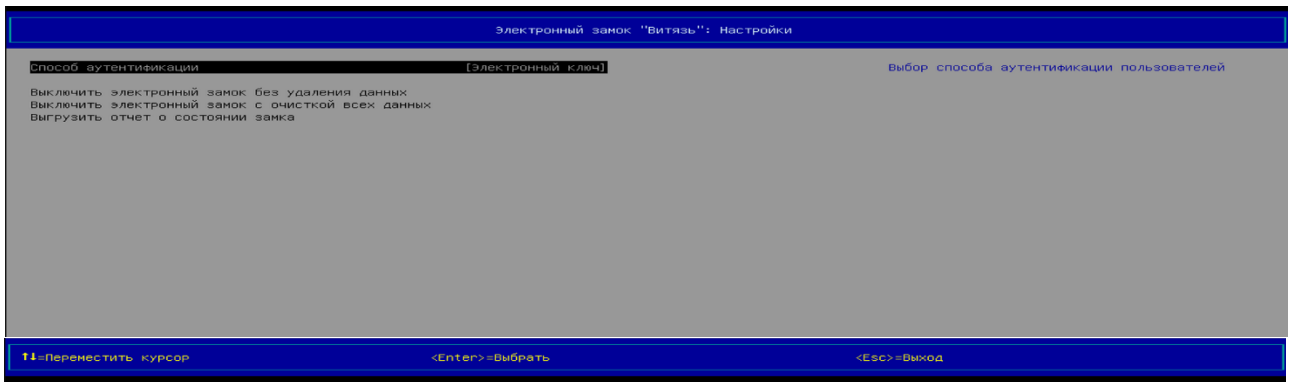


Рис. 17

3. После включения ПК «ЭЗ «ВИТЯЗЬ» 2.2 отображение статуса модуля *Электронный замок «Витязь»* меняется с «Выкл» на «Вкл» на странице *Настройки* (рис. 19).

4. Настоятельно рекомендуется создать профиль для второго администратора (второй профиль с ролью «администратор»). Вторым профилем с ролью «администратор» можно воспользоваться при невозможности аутентификации для входа в ПК «ЭЗ «ВИТЯЗЬ» 2.2 при использовании первого профиля с ролью «администратор», например, если: АН первого администратора инициализировано или испорчено, или утеряно.

5.3.2. Включение ПК «ЭЗ «ВИТЯЗЬ» 2.2. Метод 2

Для включения ПК «ЭЗ «ВИТЯЗЬ» 2.2 после его выключения без удаления данных следует:

1) выбрать п. *Настройки* раздела *Конфигурация* главного меню KSS;

2) нажать клавишу [Enter], отображается страница *Настройки* (рис. 6);

3) выбрать п. *Электронный замок «Витязь»* раздела *Настройки модулей безопасности*;

4) нажать клавишу [Enter], отображается страница *Электронный замок «Витязь», Настройки* с пунктом включения ПК «ЭЗ «ВИТЯЗЬ» 2.2 (рис. 10);

5) нажать клавишу [Enter], отображается диалоговое окно (рис. 11), запрашивающее подтверждение на включение ПК «ЭЗ «ВИТЯЗЬ» 2.2;

6) нажать клавишу [Enter], отображается страница *Локальная аутентификация* (при включении ПК «ЭЗ «ВИТЯЗЬ» 2.2 после его выключения без удаления данных, сверху есть информация об ограничении доступа: *«Ограничение доступа: Включение замка. Доступ разрешен только администратору»)*, в которой администратору предлагается подключить АН к USB-порту;

7) для прохождения аутентификации:

– если до выключения ПК «ЭЗ «ВИТЯЗЬ» 2.2 без удаления данных, в его настройках был выбран способ аутентификации пользователя по электронному ключу, то подключить АН к USB-порту, после обнаружения системой подключенного АН ввести пароль пользователя;

– если до выключения ПК «ЭЗ «ВИТЯЗЬ» 2.2 без удаления данных, в его настройках был выбран способ аутентификации пользователя по цифровому сертификату или цифровому сертификату и электронному ключу, то подключить АН к USB-порту, после обнаружения системой подключенного АН, ввести пароль пользователя, осуществляется поиск сертификатов пользователей, расположенных на АН, после завершения поиска сертификатов выбрать требуемое значение ключевого поля *Общее имя (CN)* одного из найденных сертификатов, выбрать значение ключевого поля;

8) нажать клавишу [Enter], отображается страница *Лицензионное соглашение* (рис. 12);

9) нажать клавишу [Enter], отображается страница *Электронный замок «Витязь», Настройки* (рис. 13).

Примечание. После включения ПК «ЭЗ «ВИТЯЗЬ» 2.2 отображение статуса модуля *Электронный замок «Витязь»* изменяется с «Выкл» на «Вкл» на странице *Настройки* (рис. 19).

5.3.3. Выключение без удаления данных (временная деактивация) ПК «ЭЗ «ВИТЯЗЬ» 2.2

Для выключения ПК «ЭЗ «ВИТЯЗЬ» 2.2 без очистки данных следует:

1) выбрать п. *Настройки* раздела *Конфигурация* главного меню KSS;

2) нажать клавишу [Enter], отображается страница *Настройки* (см. рис. 19);

3) выбрать п. *Электронный замок «Витязь»* раздела *Настройки модулей безопасности*;

4) нажать клавишу [Enter], отображается страница *Электронный замок «Витязь»: Настройки* (см. рис. 13, 17);

5) выбрать п. *Временно выключить электронный замок*;

6) нажать клавишу [Enter], отображается окно (рис. 18), запрашивающее подтверждение на выключение ПК «ЭЗ «ВИТЯЗЬ» 2.2;

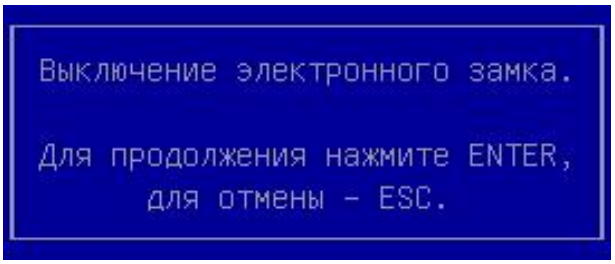


Рис. 18

7) нажать клавишу [Enter], происходит выключение ПК «ЭЗ «ВИТЯЗЬ» 2.2 без удаления ранее введенных данных (информация о пользователях, журнал событий), значения параметров настроек не изменяются на значения по умолчанию, отображение статуса модуля на странице *Настройки* изменяется с «Вкл» на «Выкл», отображается страница *Настройки*.

5.3.4. Выключение ПК «ЭЗ «ВИТЯЗЬ» 2.2 с очисткой всех данных

Для выключения ПК «ЭЗ «ВИТЯЗЬ» 2.2 с очисткой всех данных следует:

1) выбрать п. *Настройки* раздела *Конфигурация* главного меню KSS;

2) нажать клавишу [Enter], отображается страница *Настройки* (рис. 19);

Страница *Настройки* (вид 2), все модули безопасности включены

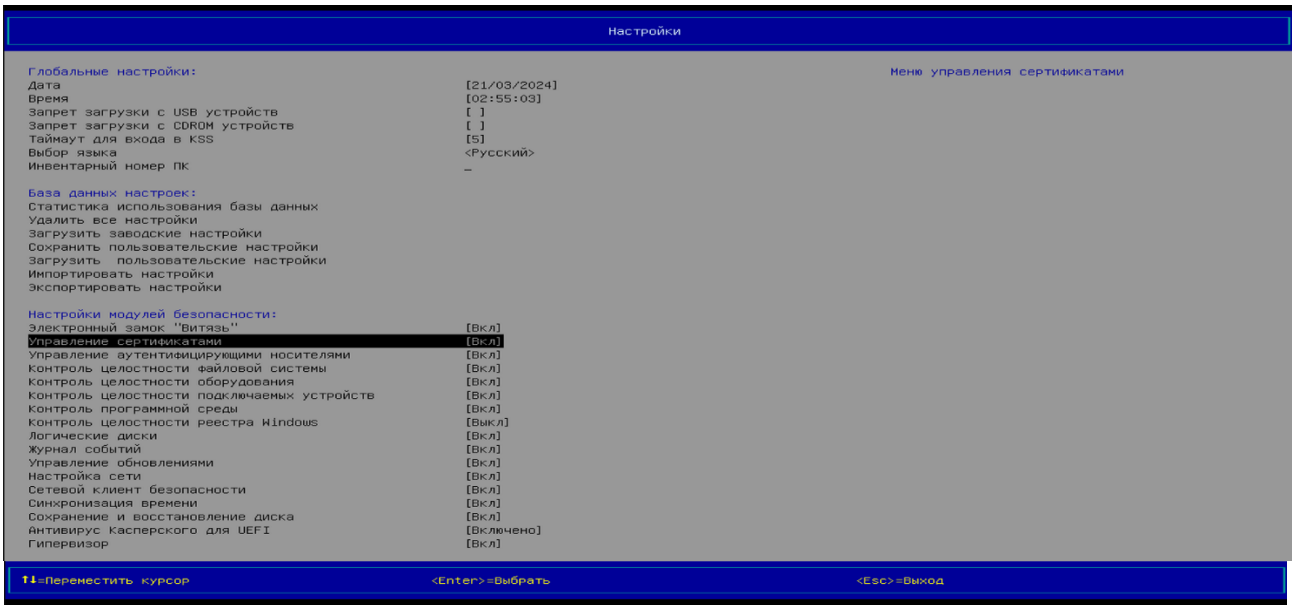


Рис. 19

3) выбрать п. *Электронный замок «Витязь»* раздела *Настройки модулей безопасности*;

4) нажать клавишу [Enter], отображается страница *Электронный замок «Витязь»: Настройки* (см. рис. 17);

5) выбрать п. *Выключить электронный замок с очисткой всех данных*;

6) нажать клавишу [Enter], отображается окно (рис. 20), запрашивающее подтверждение на выключение ПК «ЭЗ «ВИТЯЗЬ» 2.2 с очисткой всех данных;

Рис. 20

7) нажать клавишу [Enter], происходит выключение ПК «ЭЗ «ВИТЯЗЬ» 2.2 с удалением ранее введенных данных (информация о пользователях, журнал событий ПК «ЭЗ «ВИТЯЗЬ» 2.2), параметрам настроек присваиваются значения по умолчанию, отображается страница *Настройки,* отображение статуса модуля меняется с «Вкл» на «Выкл» (см. рис. 19).

5.4. Настройка параметров ПК «ЭЗ «ВИТЯЗЬ» 2.2

Настройка параметров ПК «ЭЗ «ВИТЯЗЬ» 2.2 осуществляется согласно политике безопасности, принятой в эксплуатирующей организации.

5.4.1. Максимальное количество попыток идентификации

Администратору предоставляется возможность установки максимального допустимого количества последовательных попыток идентификации пользователя.

Под максимальным допустимым количеством последовательных попыток идентификации пользователя следует понимать максимальное допустимое количество последовательных подключений (путем перебора) АН пользователя к USB-порту. После превышения данного количества попыток выполняется автоматическая перезагрузка ОС.

Для установки максимального количества попыток идентификации следует:

1) выбрать п. *Электронный замок «Витязь»* главного меню KSS (см. рис. 2);

2) нажать клавишу [Enter], отображается страница *Электронный замок «Витязь»* (рис. 21);

Страница *Электронный замок «Витязь»*

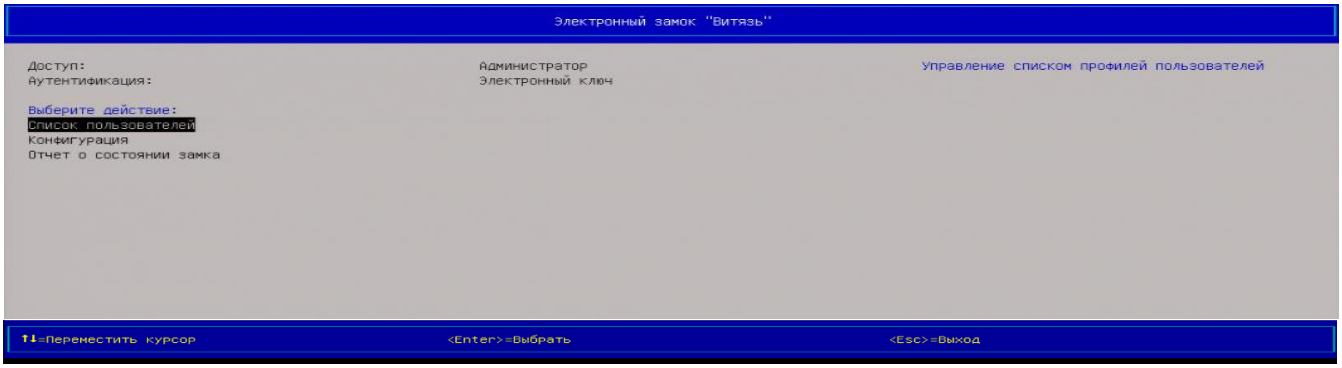


Рис. 21

3) выбрать п. *Конфигурация* раздела *Выберите действие*;

4) нажать клавишу [Enter], отображается страница *Конфигурация* (рис. 22);

Страница *Конфигурация*, п. *Максимальное количество попыток идентификации*

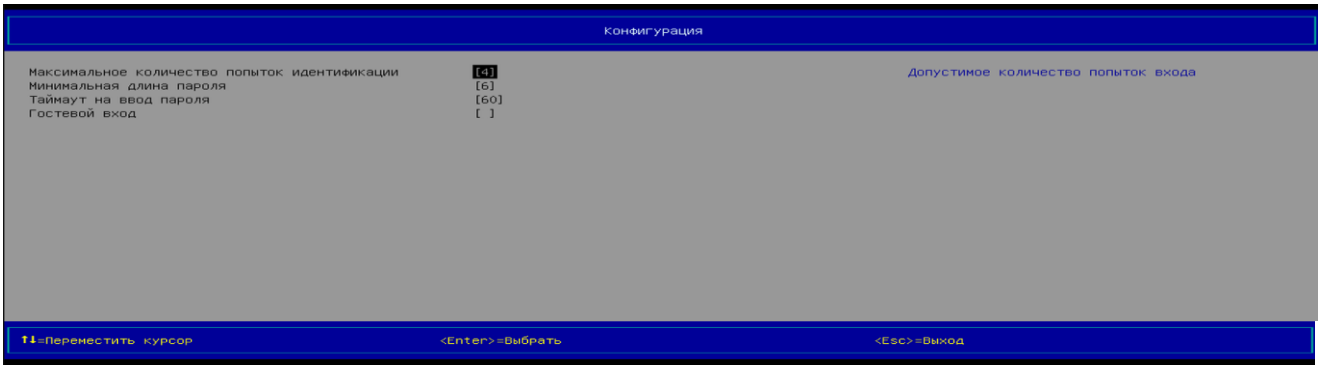


Рис. 22

5) выбрать п. *Максимальное количество попыток идентификации*;

6) нажать клавишу [Enter] и установить требуемое максимально допустимое количество попыток идентификации клавишами на цифровом блоке клавиатуры;

7) нажать клавишу [Esc] для выхода.

Примечания:

1. Установка максимального количества попыток идентификации возможна только после включения модуля *Электронный замок «Витязь»*.

2. По умолчанию максимальное количество попыток идентификации равно 4.

3. Установить максимальное количество попыток идентификации после перехода на страницу *Конфигурация* также можно следующим образом:

– после выбора пункта нажать клавишу [Enter];

– ввести значение, используя цифровой блок клавиатуры (допустимые значения: от 1 до 8);

– нажать клавишу [Enter].

5.4.2. Минимальная длина пароля

Администратор имеет возможность установки значения минимальной длины пароля пользователя.

Для установки значения минимальной длины пароля следует:

1) выбрать п. *Электронный замок «Витязь»* главного меню KSS (см. рис. 4);

2) нажать клавишу [Enter], отображается страница *Электронный замок «Витязь»* (см. рис. 21);

3) выбрать п. *Конфигурация* раздела *Выберите действие*;

4) нажать клавишу [Enter], отображается страница *Конфигурация* (рис. 23);

Страница *Конфигурация*, п. *Минимальная длина пароля*

Рис. 23

5) выбрать п. *Минимальная длина пароля*;

6) нажать клавишу [Enter] и установить требуемое значение минимальной длины пароля клавишами на цифровом блоке клавиатуры;

7) нажать клавишу [Esc] для выхода.

Примечания:

1. Установка минимальной длины пароля возможна только после включения модуля *Электронный замок «Витязь»* (см. подраздел 5.3).

2. Значение минимально допустимой длины пароля должно быть не меньше 4 символов.

3. По умолчанию минимальная длина пароля равна 6 символам.

4. Установить значение минимальной длины пароля после перехода на страницу Конфигурация также можно следующим образом:

– после выбора пункта нажать клавишу [Enter];

– ввести значение, используя цифровой блок клавиатуры (допустимые значения: от 4 до 20);

– нажать клавишу [Enter].

5.4.3. Таймаут на ввод пароля

Для установки значения длительности ожидания (таймаута) на ввод пароля:

1) выбрать п. *Электронный замок «Витязь»* главного меню KSS (см. рис. 4);

2) нажать клавишу [Enter], отображается страница *Электронный замок «Витязь»* (см. рис. 21);

3) выбрать п. *Конфигурация* раздела *Выберите действие*;

4) нажать клавишу [Enter], отображается страница *Конфигурация* (рис. 24);

Страница *Конфигурация*, п. *Таймаут на ввод пароля*

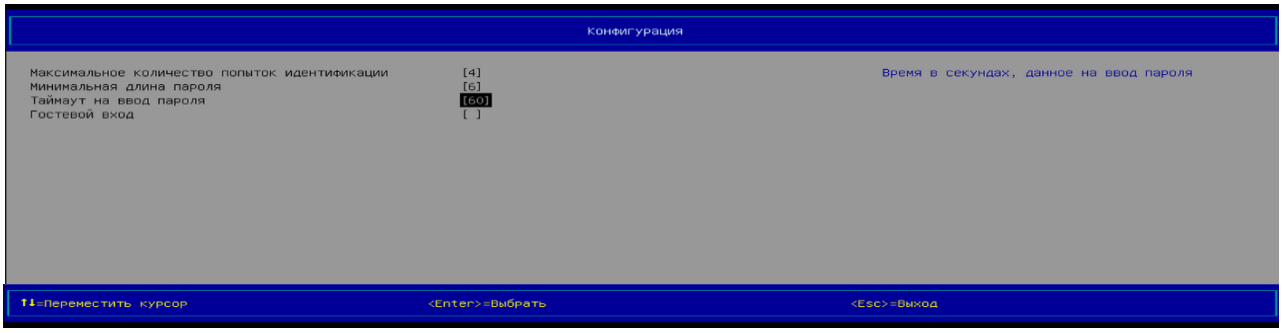


Рис. 24

5) выбрать п. *Таймаут на ввод пароля*;

6) нажать клавишу [Enter] и установить требуемое значение таймаута клавишами на цифровом блоке клавиатуры;

7) нажать клавишу [Esc] для выхода.

Примечания:

1. Установка значения таймаута на ввод пароля возможна только после включения модуля *Электронный замок «Витязь»* (см. подраздел 5.3).

2. По умолчанию значение таймаута на ввод пароля равно 60 с.

3. По истечении времени, отведенного для ввода пароля, в случае, если пароль не был введен, отображается окно с сообщением (рис. 25). Это событие будет засчитано как неудачная попытка аутентификации.

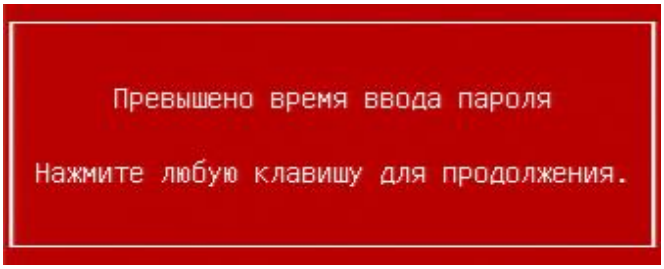


Рис. 25

4. Информация об изменении таймаута на ввод пароля записывается в журнал событий.

5. Диапазон допустимых значений таймаута на ввод пароля: от 10 до 99 с.

5.4.4. Гостевой вход

Гостевой вход предназначен для обеспечения пользователю без АН доступа к ОС компьютера. Для активации гостевого доступа:

1) выбрать п. *Электронный замок «Витязь»* главного меню KSS (см. рис. 4);

2) нажать клавишу [Enter], отображается страница *Электронный замок «Витязь»* (см. рис. 21);

3) выбрать п. *Конфигурация* раздела *Выберите действие*;

4) нажать клавишу [Enter], отображается страница *Конфигурация* (рис. 26);

5) выбрать п. *Гостевой вход* и нажать клавишу [Enter]

Страница *Конфигурация*, п. *Гостевой вход*

Рис. 26

6) выбрать п. *Таймаут на гостевой вход* и нажать клавишу [Enter];

7) нажать клавишу [Enter] и установить требуемое значение таймаута на гостевой вход клавишами на цифровом блоке клавиатуры;

8) нажать клавишу [Esc] для выхода.

5.5. Контроль целостности ПК «ЭЗ «ВИТЯЗЬ» 2.2 перед началом работы с ним пользователей

При первом запуске компьютера, при появлении окна *Приглашение на вход в KSS* (см. рис. 1) следует:

1) нажать клавишу [F1] для входа в оболочку KSS, отображается страница *Kraftway Secure Shell*;

2) провести настройку основных параметров ПК «ЭЗ «ВИТЯЗЬ» 2.2 (см. подраздел. 5.4);

3) создать профиль первого администратора;

4) данному администратору перейти на страницу *Контроль модулей безопасности* и провести сверку отображенных контрольных сумм (КС) модуля *Электронный замок «Витязь»* (файл TrustedBoot.efi), других модулей безопасности и драйверов ПК «ЭЗ «ВИТЯЗЬ» 2.2 с контрольной суммой (КС) файлов, приведенными в формуляре на ПК «ЭЗ «ВИТЯЗЬ» 2.2 (643.18184162.00006-02 30);

5) совпадение КС свидетельствует о целостности поставленного ПК «ЭЗ «ВИТЯЗЬ» 2.2.

6. ПРОЦЕДУРЫ УСТРАНЕНИЯ НЕДОСТАТКОВ. ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

6.1. Обязательства по технической поддержке ПК «ЭЗ «ВИТЯЗЬ» 2.2

Предприятие-изготовитель принимает на себя обязательства по технической поддержке ПК «ЭЗ «ВИТЯЗЬ» 2.2 изделия в полном объеме.

В период оказания технической поддержки предприятие-изготовитель гарантирует выполнение ПК «ЭЗ «ВИТЯЗЬ» 2.2 функций по назначению ПК «ЭЗ «ВИТЯЗЬ» 2.2, при соблюдении потребителем (заказчиком) требований по эксплуатации, изложенных в ЭД.

Использование ПК «ЭЗ «ВИТЯЗЬ» 2.2 после прекращения технической поддержки не допускается.

Предприятие-изготовитель принимает на себя обязательства по поиску ошибок реализации и уязвимостей в ПК «ЭЗ «ВИТЯЗЬ» 2.2 на протяжении срока действия технической поддержки, а также обязательства по своевременному информированию потребителя (заказчика) о найденных ошибках и уязвимостях.

При возникновении проблем, связанных с работой ПК «ЭЗ «ВИТЯЗЬ» 2.2, а также для получения консультации потребитель (заказчик) может круглосуточно обращаться в контакт-центр технической поддержки АО «Крафтвэй корпорэйшн ПЛС»:

1) по телефонам:

– 8 (495) 969-24-04 – для Москвы;

– 8 (800) 200-03-55 – для регионов;

2) по электронной почте: support@kraftway.ru;

3) через интернет-форму по адресу: https://www.kraftway.ru/support/support.php.

6.2. Регламент информирования о выявленных уязвимостях

В случае обнаружения уязвимости, предприятие-изготовитель распространяет обновление безопасности потребителям (заказчикам). Для этого предприятие-изготовитель:

1) доводит до потребителя (заказчика) информацию о наличии уязвимости и способах ее устранения путем рассылки по электронной почте с адреса support@kraftway.ru и публикации на своем веб-сайте на странице https://www.kraftway.ru/support/support.php.

2) выпускает обновление ПК «ЭЗ «ВИТЯЗЬ» 2.2 и проводит в установленном порядке сертификационные испытания обновления;

3) размещает обновление безопасности, измененную ЭД, обновленный сертификат соответствия (в случае переоформления) на странице по адресу: https://www.kraftway.ru/support/support.php.

При получении указанной информации потребитель (заказчик) должен руководствоваться информацией, приведенной в строке «Получение и применение» таблицы 1.

7. РЕГЛАМЕНТ ОБНОВЛЕНИЯ ПК «ЭЗ «ВИТЯЗЬ» 2.2 ПОТРЕБИТЕЛЕМ

Для поддержания ПК «ЭЗ «ВИТЯЗЬ» 2.2 в сертифицированном статусе уполномоченный администратор должен не реже одного раза в полгода ознакомиться с информацией об обновлении ПК «ЭЗ «ВИТЯЗЬ» 2.2.

Информация об обновлении ПК «ЭЗ «ВИТЯЗЬ» 2.2, а также о статусе сертификата и сроках технической поддержки ПК «ЭЗ «ВИТЯЗЬ» 2.2, сертифицированного в Системе сертификации ФСТЭК России, размещена на сайте предприятия-изготовителя по адресу: https://www.kraftway.ru/support/podderzka-po.

Для ПК «ЭЗ «ВИТЯЗЬ» 2.2 определены три типа обновления:

1) обновление антивирусных баз для модуля *Антивирус Касперского для UEFI,* осуществляемое локально администратором, в месте размещения компьютера, в состав которого входит ПК «ЭЗ «ВИТЯЗЬ» 2.2 (данное обновление не изменяет сам ПК «ЭЗ «ВИТЯЗЬ» 2.2);

2) очередное (плановое) обновление для расширения и (или) совершенствования функционала ПК «ЭЗ «ВИТЯЗЬ» 2.2 (см. подраздел. 7.1);

3) внеочередное (оперативное) обновление для блокирования возможных уязвимостей (см. подраздел. 7.2).

ВАЖНО! ЗАМЕНА ИЛИ ОБНОВЛЕНИЕ ПК «ЭЗ «ВИТЯЗЬ» 2.2 ОСУЩЕСТВЛЯЕТСЯ ТОЛЬКО НА ПРЕДПРИЯТИИ-ИЗГОТОВИТЕЛЕ СОГЛАСНО УСТАНОВЛЕННОМУ РЕГЛАМЕНТУ (СМ. ПОДРАЗДЕЛ 7.1).

ВАЖНО! КС ОБЪЕКТНЫХ ФАЙЛОВ ОБНОВЛЕННОГО ПК «ЭЗ «ВИТЯЗЬ» 2.2 УТОЧНЯЮТСЯ В ФОРМУЛЯРЕ ПОСЛЕ ЗАВЕРШЕНИЯ ПРОЦЕДУРЫ ОБНОВЛЕНИЯ.

Этапы жизненного цикла обновлений ПК «ЭЗ «ВИТЯЗЬ» 2.2 приведены в таблице 1.

Таблица 1 – Этапы жизненного цикла обновлений ПК «ЭЗ «ВИТЯЗЬ» 2.2

Этап	Тип 1	Тип 2 (плановый)	Тип 3 (оперативный)
Выпуск	Согласно установленной предприятием-изготовителем процедуре, вплоть до окончания срока поддержки	Согласно плану предприятия-изготовителя	При возникновении необходимости
Публикация	Непосредственно после выпуска	По прохождении сертификационных испытаний	Непосредственно после выпуска
Сертификационные испытания	Не выполняется	После выпуска – в срок, предусмотренный предприятием-изготовителем	После выпуска – в срок, предусмотренный предприятием-изготовителем

Этап	Тип 1	Тип 2 (плановый)	Тип 3 (оперативный)
Уведомление	Реализовано в модуле ПК «ЭЗ «ВИТЯЗЬ» 2.2	По электронной почте зарегистрированным пользователям*, на сайте предприятия-изготовителя** – в срок не позднее 5 суток после получения сертификата	По электронной почте зарегистрированным пользователям*, на сайте предприятия-изготовителя** – в срок не позднее 5 суток
Получение и применение	В соответствии с ЭД	По усмотрению потребителя (заказчика), обновление на предприятии-изготовителе	По усмотрению потребителя (заказчика), обновление на предприятии-изготовителе
* Уведомления о публикации планового и (или) оперативного обновления рассылаются по адресам электронной почты, указанным при заказе ПК «ЭЗ «ВИТЯЗЬ» 2.2. ** https://www.kraftway.ru/support/support.php .			

7.1. Плановое обновление потребителем

Порядок планового обновления ПК «ЭЗ «ВИТЯЗЬ» 2.2 потребителем следующий:

1) получение уведомления о публикации планового обновления с адреса электронной почты, указанного при заказе ПК «ЭЗ «ВИТЯЗЬ» 2.2 у предприятия-изготовителя. При неполучении уведомления рекомендуется оформить подписку на рассылку информации об обновлениях и поддержке заказанного ПК «ЭЗ «ВИТЯЗЬ» 2.2, сертифицированного в Системе сертификации ФСТЭК России. Подписка осуществляется на сайте предприятия-изготовителя по адресу: https://www.kraftway.ru/support/podderzka-po кнопкой [Подписаться на рассылку]. Следует заполнить открывшуюся форму и нажать кнопку [Отправить];

2) при желании потребителя провести обновление - согласование порядка и сроков проведения мероприятия по установке планового обновления ПК «ЭЗ «ВИТЯЗЬ» 2.2 на предприятии-изготовителе;

3) установка планового обновления ПК «ЭЗ «ВИТЯЗЬ» 2.2 на компьютер потребителя (заказчика) на предприятии-изготовителе с последующим сравнением КС объектных файлов обновленного ПК «ЭЗ «ВИТЯЗЬ» 2.2 с новыми значениями КС, приведенными в формуляре.

Примечание. Описание последовательности действий для отображения КС установленных объектных файлов ПК «ЭЗ «ВИТЯЗЬ» 2.2 дано в подразделе 5.3.

7.2. Меры блокирования возможных уязвимостей (оперативное обновление)

Работы по выявлению и устранению уязвимостей проводятся непрерывно и предусматривают выпуск оперативного обновления, основанием для которого является подтвержденная информация о наличии уязвимости в ПК «ЭЗ «ВИТЯЗЬ» 2.2. Установка оперативного обновления выполняется на предприятии-изготовителе. Опубликованные

оперативные обновления включаются в дальнейшем в состав очередного, планового обновления ПК «ЭЗ «ВИТЯЗЬ» 2.2.

Получение информации об уязвимостях осуществляется с использованием данных, поступающих из следующих источников:

1) общедоступная база уязвимостей (CVE) по адресу: http://cve.mitre.org;

2) банк данных угроз безопасности информации ФСТЭК России по адресу: https://bdu.fstec.ru;

3) форма обратной связи на сайте предприятия-изготовителя: https://www.kraftway.ru.

Доступ к форме обратной связи *Подписаться на рассылку об уязвимостях* осуществляется следующим образом:

1) перейти на сайт по адресу: https://www.kraftway.ru;

2) выбрать в меню Продукты > Программное обеспечение > Средства защиты информации;

3) выбрать на ленте слайд «Программный комплекс электронный замок «Витязь»;

4) нажать кнопку [Подписаться на рассылку], заполнить форму, нажать кнопку [Отправить].

Порядок взаимодействия при выявлении возможных уязвимостей в ПК «ЭЗ «ВИТЯЗЬ» 2.2 следующий:

1) информирование предприятие-изготовителя через форму обратной связи сайта предприятия-изготовителя или по электронной почте на адрес support@kraftway.ru о возникших проблемах;

2) подтверждение предприятием-изготовителем наличия проблем по электронной почте с адреса support@kraftway.ru;

3) при желании потребителя провести обновление - согласование порядка и сроков проведения мероприятия по установке оперативного обновления ПК «ЭЗ «ВИТЯЗЬ» 2.2 с предприятием-изготовителем;

4) установка оперативного обновления на компьютер потребителя (заказчика) на предприятии-изготовителе с последующим сравнением КС объектных файлов обновленного ПК «ЭЗ «ВИТЯЗЬ» 2.2 с новыми значениями КС, приведенными в формуляре.

Примечание. Описание последовательности действий для отображения КС установленных объектных файлов ПК «ЭЗ «ВИТЯЗЬ» 2.2 дано в подразделе 5.3.

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

Сокращение	Наименование
АН	Аутентифицирующий носитель
КС	Контрольная сумма
КЦ	Контроль целостности
ОС	Операционная система
ПК	Программный комплекс
ПО	Программное обеспечение
САВЗ	Средство антивирусной защиты
СДЗ	Средство доверенной загрузки
ЭД	Эксплуатационная документация
ЭЗ	Электронный замок
BIOS	англ. Basic Input/Output System – базовая система ввода/вывода
CDROM	англ. Compact Disc Read-Only Memory – разновидность компакт-дисков с записанными на них данными, доступными только для чтения
CN	англ. Common Name – общее имя
EXT	англ. Extended File System – расширенная файловая система в ОС Linux
FAT	англ. File Allocation Table – файловая система ОС MS-DOS, Windows 9x
KSS	англ. Kraftway Secure Shell – оболочка для управления модулями безопасности
NTFS	англ. New Technology File System – файловая система новой технологии, основная файловая система в ОС Windows
NTP	англ. Network Time Protocol – протокол сетевого времени
PIN-код	англ. Personal Identification Number – персональный идентификационный номер, аналог пароля
SPI	англ. Serial Peripheral Interface – синхронный последовательный интерфейс связи
SPI Flash	Микросхема памяти для хранения внутреннего ПО материнской платы
UEFI	англ. Unified Extensible Firmware Interface – интерфейс между ОС и микропрограммами, управляющими низкоуровневыми функциями оборудования
UPN	англ. Universal Program Name – универсальное программное имя
USB	англ. Universal Serial Bus – универсальная последовательная шина

Лист регистрации изменений									
Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					