

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ  
по защите служебной информации от несанкционированного доступа  
в Военно-космической академии имени А.Ф.Можайского

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Методические рекомендации (далее – Рекомендации) разработаны в соответствии с требованиями Федерального закона Российской Федерации «Об информации, информационных технологиях и о защите информации»<sup>1</sup> и Руководства по защите информации от несанкционированного доступа в Вооруженных Силах Российской Федерации<sup>2</sup>, Инструкции по организации в Вооруженных Силах Российской Федерации защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, обрабатываемой в государственных информационных системах и информационных системах персональных данных<sup>3</sup> и устанавливают единый порядок организации защиты информации<sup>4</sup> от несанкционированного доступа на объектах информатизации (информационных системах), не обрабатывающих сведения, составляющие государственную тайну, в Военно-космической академии имени А.Ф.Можайского (далее – академия) и определяют основные требования по безопасности информации, обрабатываемой с использованием средств вычислительной техники.

Положения Рекомендаций обязательны к исполнению всеми должностными лицами академии.

2. В Рекомендациях используются следующие основные понятия:

**автоматизированная система (АС)** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;

**автоматизированное рабочее место (АРМ)** – программно-технический комплекс АС, предназначенный для автоматизации деятельности определенного вида.

**администратор безопасности** – должностное лицо, ответственное за защиту автоматизированной (информационной) системы от несанкционированного доступа к информации;

**аутентификация** – проверка принадлежности субъекту доступа (пользователю) предъявленного им идентификатора (ключа или пароля), подтверждение подлинности;

**идентификация** – процесс распознавания пользователей путем присвоения им уникальных меток (идентификаторов);

**безопасность информации** – состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной (информационной) системой, от внутренних или внешних угроз;

**доступ к информации** – ознакомление с информацией, ее обработка, в частности копирование, модификация или уничтожение информации;

**защита информации (ЗИ)** – деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;

**защищаемая информация** – информация подлежащая защите в соответствии с требованиями правовых документов;

1 Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ.

2 Утверждено приказом Министра обороны Российской Федерации 2013 года № 011.

3 Утверждена приказом Министра обороны Российской Федерации 2014 года № 925дсп.

4 В тексте Рекомендаций под служебной информацией понимается несекретная служебная информация и информация ограниченного распространения с пометкой «Для служебного пользования», обрабатываемая на СВТ в подразделениях академии.

**информационные ресурсы** – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах), а также машинные носители информации (жесткие магнитные диски, оптические диски и т.п.);

**информационная система (ИС)** – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

**информационно-телекоммуникационная сеть (ИТКС)** – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

**информационно-телекоммуникационная сеть общего пользования (ИТКС ОП)<sup>1</sup>** – информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано;

**компрометация** – факт доступа постороннего лица к защищаемой информации, а также подозрение на него. Под компрометацией понимаются утрата, хищение, разглашение, захват или другие происшествия с идентификаторами доступа и паролями пользователей.

**компьютерная атака** – целенаправленное воздействие на автоматизированные (информационные) системы и информационно-телекоммуникационные сети программно-техническими средствами, осуществляемое в целях нарушения безопасности информации в этих системах и сетях;

**машинный носитель информации (МНИ)** – материальный носитель, содержащий информацию, представленную в форме, приспособленной для обработки с использованием средств вычислительной техники;

**мероприятия по защите информации** – совокупность действий, направленных на разработку и (или) практическое применение способов и средств защиты информации;

**несанкционированный доступ (НСД) к информации** – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами ВТ или автоматизированных систем;

**объект информатизации** – совокупность информационных ресурсов, основных технических средств и систем обработки информации, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, средств) академии, в которых они установлены;

**обработка информации** – совокупность операций сбора, накопления, ввода-вывода, приема-передачи, записи, хранения, регистрации, уничтожения, преобразования и отображения, осуществляемых над информацией;

**орган обеспечения безопасности информации (орган ОБИ)** – (отдельные должности) в службе защиты государственной тайны, предназначенные для выполнения комплекса мероприятий по созданию и поддержанию требуемого уровня безопасности информации при ее обработке с использованием СВТ академии. Является штатным органом ОБИ;

**ответственный за защиту информации** – отдельное должностное лицо, назначенное приказом начальника ответственным за защиту информации на объекте информатизации подразделения для практического выполнения комплекса мероприятий по созданию и поддержанию требуемого уровня безопасности информации при ее обработке с использованием средств ВТ подразделения. Является штатным органом ОБИ;

**пользователь (потребитель) информации** – субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;

**средства защиты информации (СЗИ)** – технические, криптографические, программные и другие средства, предназначенные для защиты информации, средства, в

<sup>1</sup> Примерами ИТКС ОП являются: сеть Интернет, региональные сети передачи данных, сети операторов связи и т. п.

которых они реализованы, а также средства контроля эффективности защиты информации;

**средства вычислительной техники (СВТ)** – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем;

**средства антивирусной защиты информации (САЗ)** – программное средство, предназначенное для обнаружения (выявления) и уничтожения вредоносных программ.

**база вирусных сигнатур (БВС)** – база известных программных кодов (сигнатур) вирусов, составляемая и регулярно обновляемая разработчиками САЗ и используемая САЗ для обнаружения вирусов методом поиска соответствия кода просматриваемой программы сигнатурам вирусов;

**система защиты информации (система ЗИ)** – совокупность объектов информатизации, пользователей, штатных и нештатных органов ОБИ, используемых ими организационных мер и комплексов средств ЗИ, организованная и функционирующая по правилам, установленным правовыми актами Министерства обороны;

**файл регистрации, протокол, журнал или лог (log-файл)** – файл с записями о событиях в хронологическом порядке, в которых протоколируются определенные действия пользователей или программ на СВТ.

3. Целью проводимых в академии мероприятий по ЗИ является обеспечение ее безопасности.

Основными мероприятиями по ЗИ являются:

определение ответственности и обязанностей начальников всех степеней и пользователей за организацию и выполнение требований безопасности информации при использовании СВТ;

разработка (планирование) и выполнение мероприятий по ЗИ. Соблюдение должностными лицами академии требований правовых актов Министерства обороны Российской Федерации по ЗИ и обеспечению безопасности информации;

назначение ответственных за ЗИ в подразделениях академии;

подготовка (обучение) должностных лиц в области ЗИ;

учет машинных носителей информации;

определение объектов защиты, защищаемых ресурсов, круга пользователей и режима обработки защищаемой информации;

разработка разрешительной системы доступа к защищаемой информации и СВТ;

применение организационных мер и средств ЗИ;

установление ограничений на использование ИТКС ОП;

обеспечение выполнения технических и административных регламентов при выполнении работ по техническому обслуживанию СВТ;

проведение анализа эффективности применяемых мер и средств ЗИ, разработка предложений по их совершенствованию;

контроль соблюдения требований по безопасности информации должностными лицами академии, правильного функционирования средств ЗИ и своевременного устранения выявленных недостатков.

4. Для обеспечения безопасности информации, обрабатываемой с использованием СВТ, на объектах информатизации академии создается система ЗИ.

Система ЗИ должна обеспечивать безопасность обрабатываемой информации во всех структурных элементах и в режимах функционирования СВТ.

5. Используемые на объектах информатизации средства ЗИ, программные (программно-аппаратные) средства, имеющие в своем составе средства, реализующие отдельные функции ЗИ, должны быть сертифицированы в системе сертификации средств ЗИ Министерства обороны Российской Федерации по требованиям безопасности информации<sup>1</sup>.

---

<sup>1</sup> Перечень средств ЗИ, сертифицированных в Министерстве обороны Российской Федерации по требованиям безопасности информации, доводится отдельно Восьмым управлением Генерального штаба Вооруженных Сил Российской Федерации.

## II. ОБЯЗАННОСТИ ПО ОРГАНИЗАЦИИ И ОСУЩЕСТВЛЕНИЮ МЕРОПРИЯТИЙ ПО ЗИ, ОБРАБАТЫВАЕМОЙ С ИСПОЛЬЗОВАНИЕМ СВТ

6. Руководство организацией и обеспечением ЗИ от НСД, криптографической и антивирусной ЗИ в академии осуществляет начальник академии через службу защиты государственной тайны академии (далее – служба ЗГТ), которая является штатным органом ОБИ академии и имеет право давать указания структурным подразделениям академии по специальным вопросам.

Служба ЗГТ:

- координирует работу по ЗИ, обрабатываемой с использованием СВТ в академии;
- планирует мероприятия по ЗИ от НСД, обрабатываемой на объектах информатизации академии;

- организует антивирусную ЗИ в академии;

- руководит в специальном отношении ответственными за ЗИ в подразделениях академии;

- определяет потребности в средствах ЗИ (ключевых документах к ним), и организует обеспечение ими подразделений академии;

- оказывает методическую помощь подразделениям академии и участвует в организации и проведении расследований по фактам НСД к информации.

Свою деятельность по ЗИ служба ЗГТ осуществляет через начальников объектов информатизации и ответственных за ЗИ в подразделениях академии.

7. Ответственность за организацию и обеспечение ЗИ, обрабатываемой с использованием СВТ, в подразделениях академии возлагается на начальников подразделений.

Начальник подразделения **обязан**:

- знать требования нормативных правовых актов Министерства обороны Российской Федерации по ЗИ и применению эксплуатируемых в подразделении объектов информатизации (СВТ);

- знать фактическое состояние работы по ЗИ в подчиненном подразделении;

- организовывать работу по выполнению мероприятий по ЗИ и контроль их выполнения;

- формировать у подчиненных военнослужащих и гражданского персонала чувство ответственности за безопасность информации, принимать меры дисциплинарного воздействия к нарушителям требований безопасности информации;

- организовывать разработку проектов приказов начальника академии по вводу в эксплуатацию объектов информатизации в подчиненных подразделениях.

8. Начальники подразделений, эксплуатирующих объекты информатизации (применяющих СВТ) являются начальниками данных объектов информатизации.

Начальники объектов информатизации **ОБЯЗАНЫ**:

- устанавливать персональную ответственность должностных лиц за эксплуатацию конкретных технических, программных средств и информационных ресурсов, определять порядок формирования и использования информационных ресурсов;

- контролировать установленный порядок обращения с МНИ, использования информационных ресурсов, своевременное стирание информации, не предназначенной для дальнейшего использования, выполнение мероприятий по защите СВТ от компьютерных вирусов;

- инструктировать подчиненных должностных лиц по требованиям безопасности информации, установленным правовыми актами Минобороны России;

- организовывать специальную подготовку подчиненных должностных лиц по вопросам ЗИ.

9. В каждом подразделении академии, применяющем (эксплуатирующем) КСА АС или СВТ, из числа наиболее подготовленных пользователей, начальник объекта информатизации назначает ответственного за ЗИ и ответственного за эксплуатацию программных и технических средств.

На ответственного за ЗИ **возлагаются**:

- взаимодействие по вопросам ЗИ со штатным органом ОБИ академии;

разработка организационно-планирующих документов и выполнение практических мероприятий по ЗИ на объекте информатизации;

выполнение мероприятий по ЗИ при подготовке объектов информатизации к вводу в эксплуатацию;

обеспечение антивирусной ЗИ на объектах информатизации;

обеспечение безопасности информации при подключении и использовании удаленного сегмента АП ИТКС ОП «Интернет»;

обеспечение безопасности информации при использовании систем электронного документооборота;

обеспечение безопасности информации при проведении работ по сервисному техническому обслуживанию СВТ;

выполнение функций администраторов безопасности;

генерация, распределение и контроль безопасности применения пользователями паролей и средств ЗИ (в том числе криптографических);

получение обновлений САВЗ (БВС) и их установка на всех СВТ;

обеспечение безопасного применения средств активного сетевого оборудования, выполнение работ по управлению (администрированию) средствами межсетевого экранирования, обнаружения компьютерных атак;

своевременное информирование службы ЗГТ о выявлении угроз безопасности информации для принятия необходимых мер;

выявление, реагирование и участие в устранении последствий фактов НСД к защищаемым ресурсам или воздействия компьютерных вирусов и программных средств скрытого информационного воздействия;

участие в проведении мероприятий по анализу защищенности информации, обрабатываемой на объектах информатизации;

На время убытия ответственного за ЗИ в командировку, в отпуск или по болезни, МНИ и документация по ЗИ передаются в установленном порядке другому лицу, указанному в рапорте ответственного за ЗИ при убытии.

На ответственного за эксплуатацию программных и технических средств **возлагаются:**

подготовка программных, вычислительных и информационно-справочных ресурсов для ввода в эксплуатацию комиссией академии;

участие в работе комиссии академии по вводу в эксплуатацию средств общего программного обеспечения и средств ЗИ;

контроль пользователей за эксплуатацией программных и технических средств объекта информатизации в соответствии с инструкцией по ЗИ и эксплуатационной документацией;

своевременное согласование с ответственным за ЗИ изменений, вносимых в состав программных и технических средств объекта информатизации.

10. Все лица независимо от занимаемой должности, допущенные к защищаемым ресурсам объекта информатизации, самостоятельно обрабатывающие информацию на СВТ или в чьих интересах производится ее автоматизированная обработка, являются пользователями этого объекта.

Они отвечают за соблюдение установленного порядка использования технических и программных средств и несут персональную ответственность за безопасность информации на своих АРМ.

Пользователи **обязаны:**

осуществлять работы на объектах информатизации только после их ввода в эксплуатацию в установленном порядке;

знать свои полномочия и права доступа к защищаемым ресурсам объекта информатизации;

знать и выполнять требования по ЗИ;

соблюдать установленный порядок учета, хранения и отправки МНИ;

уметь самостоятельно применять средства ЗИ и антивирусной защиты, установленные на СВТ;

знать порядок действий при стихийных бедствиях, а также при компрометации (утрате) паролей и идентификаторов доступа;

выполнять блокирование консоли или завершение открытого сеанса работы с доступом к ресурсам при необходимости временного оставления СВТ;

осуществлять визуальный контроль целостности элементов контроля НСД (наклеек, печатей, пломб, защитных знаков) к внутренним узлам и блокам СВТ;

докладывать ответственному за ЗИ о выявленных фактах или предпосылках к возникновению каналов НСД к защищаемым ресурсам или нарушении их целостности, изменениях в конфигурации технических средств и программного обеспечения, компрометации (утрате) паролей и идентификаторов доступа, воздействии (подозрении воздействия) компьютерных вирусов и программных средств скрытого информационного воздействия;

осуществлять выключение СВТ перед сдачей под охрану помещений объекта информатизации по окончании рабочего дня (если эксплуатационной документацией или организационно не предусмотрен другой режим работы).

#### **11. Пользователям запрещается:**

вносить изменения в состав, конструкцию, конфигурацию и размещение технических средств объекта информатизации;

вносить изменения в структуру файловой системы СВТ без согласования с ответственным за ЗИ, в том числе проводить работы по изменению (переустановке) программного обеспечения, системных файлов и реестров операционных систем, препятствующие выяснению причин фактов НСД к защищаемым ресурсам;

обрабатывать информацию и выполнять другие работы, не предусмотренные перечнем защищаемых ресурсов и инструкцией по ЗИ;

осуществлять попытки НСД к базам (хранилищам) данных и информации других пользователей;

открывать, пересылать, запускать приложения (прикрепленные файлы) к электронным сообщениям (письмам), полученным по системам передачи данных (электронной почты, электронного документооборота) без проверки САВЗ;

использовать сервисы передачи данных, не разрешенные эксплуатационной документацией и инструкцией по ЗИ;

осуществлять загрузку с внешних МНИ операционных систем или терминальных сред, встроенных в СВТ, если такая загрузка не предусмотрена эксплуатационной документацией или инструкцией по ЗИ;

использовать средства ЗИ (в том числе криптографические), не включенные в состав объекта информатизации в установленном порядке;

отключать (демонтировать, блокировать) средства ЗИ и регистрации информации;

записывать на какие-либо носители информации и распечатывать пароли;

проводить любые работы по исследованию (анализу) структуры файлов, содержащих компьютерные вирусы или программные средства скрытого информационного воздействия;

подключать СВТ к ИТКС ОП;

подключать к СВТ, предназначенным для работы в ИТКС ОП, МНИ, за исключением тех, которые специально выделены для этих целей;

использовать для обработки информации неучтенные МНИ, а также личные СВТ.

Должностные лица, допустившие нарушения положений настоящих Рекомендаций, привлекаются к дисциплинарной, административной или уголовной ответственности в соответствии с законодательством Российской Федерации и руководящими документами Министерства обороны Российской Федерации.

12. Допуск пользователей к обработке информации на объекте информатизации подразделения осуществляется в соответствии с перечнем защищаемых ресурсов объекта информатизации после изучения данных Рекомендаций и инструкции по ЗИ объекта информатизации (под роспись).

Подготовка должностных лиц подразделений, являющихся пользователями объектов информатизации, и обеспечивающих эксплуатацию (применение) объектов

информатизации (СВТ), планируется и осуществляется в рамках профессионально-должностной подготовки академии.

### III. ОРГАНИЗАЦИЯ ЗИ ПРИ СОЗДАНИИ И ЭКСПЛУАТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

13. В целях создания и ввода в эксплуатацию объекта информатизации подразделения академии проводятся следующие мероприятия:

определение необходимого состава оборудования, размещение (монтаж) технических средств;

разработка учетной документации ([формы №№ 8-11](#));

назначение приказом начальника академии комиссии<sup>1</sup>, которой проводится комплекс мероприятий по вводу объекта информатизации в эксплуатацию;

комиссионно определяется структура и функциональное назначение СВТ, включаемых в состав объекта<sup>2</sup>; перечень должностных лиц (пользователей и(или) групп пользователей, а также администраторов)<sup>3</sup> и их права на доступ к защищаемым ресурсам (МНИ, каталогам, файлам). На основе вышеуказанных данных составляется перечень защищаемых ресурсов ([форма № 6](#)), который уточняется ежегодно ответственным за ЗИ и при необходимости перерабатывается;

комиссионно определяются: одно- или многопользовательский режим обработки информации с равными или различными правами доступа к информации; уровень значимости обрабатываемой информации (служебная несекретная или ограниченного распространения с пометкой «Для служебного пользования»); класс защищенности в соответствии с таблицей 1 ([форма № 1](#)). На основе вышеуказанных данных составляется акт классификации объекта информатизации ([форма № 2](#));

комиссионно определяются общесистемное и специальное программное обеспечение, необходимое для решения задач по обработке информации на объекте; пользователями, совместно с ответственным за ЗИ, проводится установка программного обеспечения, информационно-справочных ресурсов, САВЗ и средств ЗИ. По результатам проведенных работ составляется акт ввода в эксплуатацию средств общего программного обеспечения и средств ЗИ ([форма № 3](#));

ответственным за ЗИ на объекте информатизации разрабатывается таблица разграничения доступа к защищаемым ресурсам объекта информатизации ([форма № 7](#));

ответственным за ЗИ проводится настройка средств ЗИ и САВЗ в соответствии с таблицей разграничения доступа, инструкциями по настройке САВЗ и средств ЗИ, а также отключение функции автозапуска внешних носителей. После настройки средств ЗИ и САВЗ комиссией проводится проверка готовности системы ЗИ объекта информатизации и составляется акт готовности системы ЗИ объекта информатизации ([форма № 4](#));

пользователями, совместно с ответственным за ЗИ, проводится опечатывание технических средств номерными металлическими печатями пользователя и ответственного за ЗИ, после чего ответственный за ЗИ разрабатывает перечень опечатываемых устройств и блоков ([форма № 16](#));

МНИ учитываются по журналу ([форма № 10](#)) (учету подлежат все МНИ, в том числе жесткие диски СВТ и принтеров, на которых они установлены), после чего оборудуются соответствующими бирками ([форма № 15](#));

корпуса СВТ оборудуются бирками установленного образца ([форма № 14](#));

<sup>1</sup> В состав комиссии включаются начальник объекта информатизации (председатель комиссии), должностное лицо ответственное за эксплуатацию программных и технических средств, ответственный за ЗИ, представитель органа ОБИ службы ЗИТ и начальник узла связи академии. Комиссия назначена приказом начальника академии от 28.04.2015 г. № 14дсп.

<sup>2</sup> Выделяются следующие типы функциональных элементов: специальная электронно-вычислительная машина (мейнфрэйм, спецвычислитель и т. п.); стационарная автономная персональная электронно-вычислительная машина (ПЭВМ); переносная автономная ПЭВМ (ноутбук, нетбук и т. д.); рабочая станция локальной вычислительной сети (ЛВС); сервер (файловый, безопасности, приложений, баз данных, печати, почтовый и т. п.).

<sup>3</sup> Если на СВТ не представляется возможным определить конкретное количество пользователей (например: компьютерные классы академии), то на каждом СВТ создаются учетные записи пользователей по категориям (например: администратор, слушатели, преподаватели, курсанты и т. п.) и оформляется «Журнал учета работы пользователей в компьютерном классе подразделения» с обязательным указанием следующих граф: № п/п, Ф.И.О., наименование учетной записи, время начало работ, время окончания работ, примечание.

ответственным за ЗИ на объекте информатизации разрабатывается инструкция по ЗИ ([форма № 22](#)) на объекте информатизации подразделения, подписывается начальником объекта информатизации, согласовывается со штатным органом ОБИ службы ЗГТ и утверждается должностным лицом, указанным в таблице 3 ([форма № 24](#));

ответственным за ЗИ на объекте информатизации разрабатывается проект приказа начальника академии о вводе объекта информатизации подразделения в эксплуатацию ([форма № 18](#)).

14. На этапе проверки готовности системы ЗИ объекта информатизации и подготовки проекта приказа начальника академии о вводе объекта информатизации в эксплуатацию комиссией, назначенной приказом начальника академии, проверяются:

полнота и качество отработки организационно-распорядительной и учетной документации;

правильность установки и настройки средств ЗИ, САВЗ и их обновления;

тестирование объекта информатизации во всех режимах функционирования;

наличие учетной записи администратора безопасности (ответственного за ЗИ).

При необходимости проводится дополнительная настройка средств ЗИ, подготовка пользователей и доработка организационно-распорядительной документации.

По результатам проверки оформляется акт готовности системы ЗИ объекта информатизации ([форма № 4](#)).

15. На основании положительных выводов акта готовности системы ЗИ начальником академии издается приказ о вводе объекта информатизации в эксплуатацию ([форма № 18](#)), в котором определяются:

наименование объекта информатизации и дата ввода в эксплуатацию;

уровень конфиденциальности обрабатываемой информации (служебная несекретная и (или) ограниченного распространения с пометкой «Для служебного пользования»);

класс защищенности объекта информатизации;

должностные лица подразделения, на которых возлагаются обязанности начальника объекта информатизации, ответственного за ЗИ; ответственного за эксплуатацию программных и технических средств;

разрешенное время работы на объекте информатизации;

периодичность контроля полноты и качества выполнения мероприятий по ЗИ.

В приложениях к приказу начальника академии о вводе объекта информатизации в эксплуатацию ([форма № 18](#)) указываются: состав объекта информатизации, перечень пользователей (логических имен), должностные лица подразделения, на которых возлагаются обязанности начальника объекта информатизации, ответственного за ЗИ, ответственного за эксплуатацию программных и технических средств. В дальнейшем уточнение состава объекта информатизации и перечень пользователей (логических имен), осуществляется ежегодно или по мере необходимости.

16. Мониторы всех СВТ объектов информатизации, не предназначенных для обработки сведений, составляющих государственную тайну, оборудуются биркой с предупредительной надписью: «**Обработка секретной информации запрещена**».

17. Допуск пользователей к обработке информации на объекте информатизации осуществляется после ввода объекта в эксплуатацию порядком, установленным настоящими Рекомендациями.

18. Типовая структура и требования к содержанию инструкции по ЗИ на объекте информатизации приведены в [форме № 22](#).

Инструкция по ЗИ разрабатывается в соответствии с требованиями настоящих Рекомендаций и инструкциями по настройке средства ЗИ и антивирусной защиты ответственным за ЗИ.

Требования инструкции по ЗИ доводятся под роспись до должностных лиц (пользователей) подразделения при первичном допуске к обработке информации на объекте информатизации и в последующем – **ежегодно**.

19. Порядок действий должностных лиц (пользователей) объекта информатизации по ЗИ при ее обработке с использованием СВТ определяется инструкцией по ЗИ на объекте информатизации.



20. Ответственному за ЗИ выдача реквизитов учетных записей, идентификаторов и паролей на доступ к защищаемым ресурсам пользователям, не изучившим требования инструкции по ЗИ, **запрещается**.

21. Планирование мероприятий по ЗИ в академии осуществляется **ежегодно**.

План мероприятий по ЗИ академии разрабатывается службой ЗГТ и включается отдельным разделом в План мероприятий ЗГТ академии на год, подписывается начальником службы ЗГТ и утверждается начальником академии. Выписки из Плана мероприятий ЗГТ на год доводятся до начальников подразделений академии.

Начальники подразделений академии устанавливают сроки и определяют персональную ответственность должностных лиц подразделения за организацию и выполнение практических мероприятий по ЗИ от НСД на эксплуатируемых в подразделении объектах информатизации.

22. Используемые на объектах информатизации программные (программно-аппаратные) средства и средства ЗИ должны обеспечивать совместную бесконфликтную работу.

На объектах информатизации использовать несертифицированные в Минобороны России по требованиям безопасности информации программные (программно-аппаратные) средства ЗИ **запрещается**.

23. Прием и ввод в эксплуатацию на объектах информатизации изделий (средств) программного обеспечения и средств ЗИ осуществляются комиссией, назначенной приказом начальника академии.

После установки и настройки программного обеспечения и средств ЗИ составляется акт ([форма № 3](#)), в котором указываются: перечень программных модулей, настроек (конфигурационных файлов, управляющих наборов данных), их функции и контрольные суммы.

Акт ввода в эксплуатацию средств общего программного обеспечения и средств ЗИ хранится у ответственного за ЗИ объекта информатизации.

24. Все программные изделия, информационные массивы (базы данных, архивы, справки и т.п.), технические средства объекта информатизации подразделения и МНИ закрепляются за должностными лицами подразделения, допущенными к эксплуатации объекта информатизации.

25. На объектах информатизации СВТ пользователей, дверцы (крышки) технологических шкафов (стоек), разъемы подключения информационных кабелей сетей связи и управления, розетки подключения к локальным вычислительным сетям, дверцы (крышки), обеспечивающие доступ к активному оборудованию кабельных сетей, и другие устройства и разъемы, бесконтрольный доступ к которым может послужить причиной возникновения каналов утечки информации или воздействия на защищаемые ресурсы, опечатываются ответственным за ЗИ.

Корпуса СВТ с установленными МНИ опечатываются печатями пользователя и ответственного за ЗИ на объекте информатизации.

СВТ, на которых обработка ведется более чем одним пользователем (компьютерные классы академии), опечатываются печатями ответственного за ЗИ и начальника объекта информатизации.

26. Перечень опечатываемых устройств и блоков на объекте информатизации ([форма № 16](#)) утверждается начальником подразделения, эксплуатирующего объект информатизации и хранится у ответственного за ЗИ. На основании указанного перечня, ответственным за ЗИ, разрабатывается схема (маршрутная карта) опечатывания устройств и блоков, в которой указываются: план расположения опечатываемых устройств и блоков; места опечатывания; номера печатей лиц, ответственных за опечатывание ([форма № 16](#)).

Соответствие печатей на технических средствах объекта информатизации перечню или схеме (маршрутной карте) опечатывания устройств и блоков ([форма № 16](#)) проверяется, не реже **одного раза в месяц**, ответственным за ЗИ. Об обнаружении несоответствия оттиска печати на СВТ немедленно докладывается начальнику объекта информатизации, после чего проводится разбирательство по данному факту.

27. Корпус каждого СВТ оборудуется табличкой установленного образца ([форма № 14](#)).

28. Независимо от способов обмена информацией в электронной форме между академией и другими органами военного управления, воинскими частями и организациями (пересылка на МНИ или передача по каналам связи) в сопроводительных письмах (бумажных или электронных) указывается категория информации<sup>4</sup> и контрольная сумма<sup>5</sup> пересылаемых файлов (наборов данных) ([форма № 20](#)).

29. Контроль доступа к техническим средствам объекта информатизации осуществляется путем визуального наблюдения за техническими средствами и наличием соответствующих оттисков печатей на них.

При обнаружении факта НСД на объекте информатизации ответственный за ЗИ должен немедленно выяснить причины его возникновения и принять меры по пресечению НСД.

Факт НСД и время его обнаружения, а также результаты анализа причин происшедшего события отмечаются в журнале учета фактов НСД и воздействия компьютерных вирусов ([форма № 8](#)) с докладом начальнику подразделения, эксплуатирующего объект информатизации и уведомлением органа ОБИ службы ЗГТ.

30. На каждом объекте информатизации должна предусматриваться автоматическая регистрация обращений пользователей к защищаемым ресурсам. Регистрация осуществляется средствами ЗИ или средствами операционных систем.

При настройке операционных систем и (или) средств ЗИ должна предусматриваться регистрация сообщений, связанных с управлением доступом, из числа автоматически генерируемых операционной системой и (или) средствами ЗИ (системными журналами операционных систем, журналами средств ЗИ, log-файлы и т.д.).

31. Файлы (наборы данных) с информацией, не предназначенной для дальнейшего использования, должны быть стерты.

Стирание информации должно производиться средствами, входящими в состав сертифицированных средств ЗИ.

Стирание информации производится пользователями, создавшими файлы или являющимися их владельцами.

Стирание файлов с МНИ при их передаче (перезакреплении СВТ с установленными МНИ) между пользователями или подразделениями академии проводится пользователями указанных МНИ под контролем ответственного за ЗИ. Факт стирания информации с МНИ отмечается в журнале учета стирания информации ([форма № 9](#)).

32. В подразделениях академии, эксплуатирующих объекты информатизации, в инструкцию по ЗИ включается раздел по действиям личного состава объекта информатизации на случай стихийного бедствия. Указанный раздел в инструкции должен отражать реальные условия расположения объекта информатизации, а также конкретные действия должностных лиц по обращению с МНИ, средствами ЗИ и технической документацией на случай стихийного бедствия.

В экстренных случаях при стихийных бедствиях начальник подразделения, эксплуатирующего указанный объект, принимает меры по обеспечению его вывоза (эвакуации) и готовит все МНИ, документы и изделия к вывозу (эвакуации).

В первую очередь вывозу (эвакуации) подлежат документы и МНИ с пометкой «Для служебного пользования».

33. Техническое обслуживание и(или) ремонт СВТ проводится в соответствии с графиком ([форма № 13](#)), утвержденным начальником объекта информатизации, или при возникновении отказов (сбоев) в работе СВТ закрепленным за ними личным составом подразделений или специалистами организаций, имеющих соответствующие лицензии (в соответствии с заключенными государственными контрактами).

<sup>4</sup> В случае, если в сопроводительных письмах (бумажных или электронных) и (или) пересылаемых файлах (наборах данных) содержится информация ограниченного распространения, то на лицевой стороне первого листа сопроводительного письма в верхнем правом углу указывается ограничительная пометка «Для служебного пользования».

<sup>5</sup> При обмене информацией между объектами информатизации, построенными на базе различных КСА или СВТ, дополнительно пересылается модуль расчета контрольных сумм по соответствующим алгоритмам. Файлам, содержащим сведения о результатах расчета контрольных сумм, присваиваются расширения, указывающие на использованный при расчете алгоритм. Например: disk.md5, доклад.crc32, svedenia.crc64 и т.п.

34. Начальники объектов информатизации, должны приниматься меры, направленные на исключение возможности ознакомления лиц, осуществляющих техническое обслуживание или ремонтные работы, с защищаемой информацией.

При проведении технического обслуживания и ремонта специалистами ремонтных организаций обработка информации запрещается. Информация, находящаяся в оперативной памяти СВТ, стирается, а МНИ извлекаются из стоек, корпусов СВТ<sup>6</sup>. О факте стирания информации делается запись в журнале учета стирания информации ([форма № 9](#)).

Вскрытие технических средств объекта информатизации для проведения технического обслуживания или ремонта осуществляется с разрешения начальника объекта информатизации, с уведомлением ответственного за ЗИ и лиц, за которыми закреплены эти средства.

О вскрытии технических средств производится запись в журнале учета фактов НСД и воздействия компьютерных вирусов ([форма № 8](#)) с указанием даты, времени и причины вскрытия, а также номера печати, которой опечатываются устройства после проведения технического обслуживания или ремонта.

Вскрытие технических средств объектов информатизации, опечатанных (опломбированных) печатями, специальными голографическими наклейками и т.п., свидетельствующими о проведении специальных проверок, осуществляется комиссией, в состав которой включаются начальник объекта информатизации, ответственный за ЗИ, ответственный пользователь и представитель органа ОБИ службы ЗГТ с составлением акта ([форма № 19](#)) и последующим опечатыванием вскрытых технических средств печатями ответственного за ЗИ и пользователя (начальника объекта информатизации).

В период гарантийных сроков вскрытие технических средств (изъятие МНИ из корпусов СВТ) осуществляется способом, не приводящим к потере гарантийных обязательств, по согласованию или в присутствии представителя организации – изготовителя (поставщика) АС или СВТ.

Ответственность за сохранность печатей на технических средствах возлагается на лиц, за которыми закреплены эти средства.

35. Для проведения технического обслуживания (ремонта) технических средств на объектах информатизации запрещается применять средства, имеющие (позволяющие) подключение к ИТКС ОП, в том числе к сети Интернет.

36. При проведении технического обслуживания (ремонта) **запрещается** передавать в ремонтные организации МНИ, узлы и блоки СВТ с элементами накопления и хранения защищаемой информации независимо от ее категории.

Вышедшие из строя МНИ, не подлежащие восстановлению, списываются с материального учета академии и уничтожаются комиссией академии в установленном порядке с составлением акта ([форма № 17](#)).

37. После окончания проведения технического обслуживания и ремонтных работ должна проводиться проверка исправности средств ЗИ в соответствии с эксплуатационной документацией на них.

38. **Ежегодно** и после каждого проведения работ по монтажу, наладке, доработке и ремонту технических или программных средств объекта информатизации комиссией, назначаемой приказом начальника академии, проводится проверка функционирования всех средств ЗИ и системы предупреждения о НСД к техническим средствам объекта информатизации. Результаты работы комиссии оформляются актом ([форма № 5](#)), в котором указываются:

состав комиссии, номер и дата приказа о назначении комиссии;

основание проведенных работ и наименование подразделений (организаций), выполнивших указанные работы;

краткое описание работ;

принятые меры по ЗИ, в том числе отключение от каналов связи (вычислительной сети) и учетные номера МНИ, использовавшихся в ходе работ;

---

<sup>6</sup> При проведении работ под контролем лица, ответственного за ЗИ на объекте информатизации, допускается МНИ из стоек не извлекать.

вывод об исправности технических средств.

39. Ремонт и уборка помещений объектов информатизации производятся в присутствии ответственных за технические средства должностных лиц с соблюдением мер, исключающих доступ посторонних лиц к техническим средствам.

40. При расформировании подразделения или изменении его дислокации, снятии со снабжения СВТ или КСА АС, на базе которых были созданы объекты информатизации в подразделении, осуществляется вывод таких объектов из эксплуатации, выгрузке (копировании) защищаемых ресурсов на внешние учетные установленным порядком МНИ, дальнейшем хранении (применении) МНИ и защищаемых ресурсов или их уничтожении (стирании).

41. Вывод из эксплуатации объектов информатизации (СВТ), на которых обрабатывалась информация ограниченного распространения с пометкой «Для служебного пользования» проводится комиссией, в состав которой включаются начальник объекта информатизации, ответственный за ЗИ, ответственный за технические и программные средства, представитель органа ОБИ службы ЗГТ и начальник узла связи академии.

В ходе работы комиссией проводятся:

выгрузка (копирование) защищаемых ресурсов на внешние МНИ;

стирание информации с МНИ;

закрытие ведением документации по ЗИ, отбор документов на уничтожение.

По результатам работы комиссии составляется акт вывода объекта информатизации (СВТ) из эксплуатации ([форма № 23](#)). Акт составляется с описанием выполненных работ и указанием МНИ, на которые проводилась выгрузка (копирование) защищаемых ресурсов. После проведения вышеуказанных работ, суточным приказом начальника академии объект информатизации выводится из эксплуатации.

Объекты информатизации (СВТ), на которых обрабатывалась служебная несекретная информация, выводятся из эксплуатации суточным приказом начальника академии.

42. Все МНИ и идентификаторы доступа, использовавшиеся в ходе эксплуатации объекта информатизации, выведенного из эксплуатации, подлежат передаче в другие подразделения академии или сдаче в подразделение академии, их выдавшее.

МНИ, применение которых в составе других СВТ и объектов информатизации является невозможным по техническим причинам (неисправности), подлежат уничтожению в установленном порядке.

#### IV. ОСОБЕННОСТИ ХРАНЕНИЯ И ОБРАЩЕНИЯ С МНИ

43. В зависимости от способа использования в составе СВТ выделяют следующие типы МНИ:

встроенные (несъемные), то есть не демонтируемые из СВТ в процессе их использования;

отчуждаемые (съемные), то есть временно подключаемые к СВТ через соответствующие устройства (адаптеры) ввода-вывода.

44. Все МНИ подлежат обязательному учету<sup>7</sup>.

Уровень конфиденциальности МНИ определяется исходя из записываемой (наносимой) на них информации (служебная несекретная или ограниченного распространения с пометкой «Для служебного пользования»).

МНИ, используемые на объектах информатизации, учитываются в журнале учета МНИ ([форма № 10](#)) до записи (нанесения) на них информации.

Портативные (переносные) СВТ (нетбуки, ноутбуки, планшеты и т.д.), имеющие встроенные МНИ, технологией изготовления которых демонтаж (отключение) этих МНИ из корпуса СВТ не предусмотрен, учитываются как МНИ. Порядок обращения с такими

<sup>7</sup> Способ нанесения и состав учетных данных МНИ должны обеспечивать его однозначную идентификацию, невозможность отторжения (стирания) или подлога.



СВТ аналогичен порядку обращения, установленному настоящими Рекомендациями для МНИ.

Перед учетом в подразделении все МНИ должны быть проверены на техническую исправность. Использование технически неисправных МНИ, а также МНИ, имеющих повреждения предохранительного корпуса (конверта), запрещается.

Проверка правильности учета и маркировки МНИ проводится путем сверки записей в журналах учета МНИ ([форма № 10](#)) с учетными данными, нанесенными непосредственно на носители, ежеквартально ответственным за ЗИ.

45. МНИ, предназначенные для нанесения на них информации, перед выдачей их пользователям маркируются проставлением штампа № 1 и заполнением его реквизитов<sup>8</sup> ([форма № 15](#)). Нанесенные данные заверяются мастичной печатью «Для пакетов» и подписью лица, производившего учет. При невозможности проставления штампа № 1 допускается нанесение учетных данных заметным красителем на самом носителе или закрепление бирки, содержащей реквизиты штампа № 1.

Маркировка несъемных дисков, магнитных запоминающих устройств (оперативных, постоянных или долговременных) осуществляется нанесением заметным красителем учетных данных на внешней стороне их корпуса.

Маркировка МНИ, в которых физический носитель информации находится в предохранительном корпусе (картридже, модуле, системном блоке и т.п.), изъятие из которого технологией использования данного типа носителя не предусмотрено, осуществляется нанесением реквизитов штампа № 1 на поверхность корпуса. Опечатывание предохранительного корпуса (картриджа, модуля, системного блока и т. п.) проводится печатями пользователя и ответственного за ЗИ.

Маркировка оптических дисков осуществляется нанесением реквизитов штампа № 1 на нерабочую поверхность диска заметным красителем (маркером).

46. Обработка и размножение (печать) документов ограниченного распространения с пометкой «Для служебного пользования» должны осуществляться на специально выделенных для этой цели СВТ объекта информатизации. Количество СВТ, на которых осуществляется размножение (печать) документов ограниченного распространения с пометкой «Для служебного пользования» определяется по решению начальника подразделения. Перед вводом в эксплуатацию, на данных СВТ должна создаваться система ЗИ, соответствующая классу защищенности 1Г.

К документам, содержащим информацию ограниченного распространения, относятся документы, содержащие несекретную информацию, касающуюся деятельности структурных подразделений академии и академии в целом, ограничения на доступ (распространение) к которой диктуются служебной необходимостью.

На служебных документах (изданиях), содержащих служебную информацию ограниченного распространения, проставляется пометка «Для служебного пользования».

Необходимость проставления пометки «Для служебного пользования» на служебных документах и изданиях, содержащих служебную информацию ограниченного распространения, определяется исполнителем и должностным лицом, подписывающим (утверждающим) служебный документ. Указанная пометка и номер экземпляра проставляются в правом верхнем углу первой страницы служебного документа, на обложке и титульном листе документа, а также на первой странице сопроводительного письма к таким документам.

Служебные документы с пометкой «Для служебного пользования» учитываются поэкземплярно по журналу учета служебных документов, а служебные издания – по журналу учета служебных изданий, как правило, отдельно от несекретной документации. При незначительном объеме таких документов разрешается вести их учет совместно с другими несекретными документами. К регистрационному номеру служебного документа добавляется пометка «дсп». На обороте последнего листа каждого экземпляра отпечатанного документа указываются количество отпечатанных экземпляров, фамилия

---

<sup>8</sup> Штамп № 1 содержит следующие реквизиты: категория информации («Несекретно» или «Для служебного пользования»), наименование структурного подразделения (служба, отдел, отделение, кафедра и т.п.), номер экземпляра, учетный номер, фамилия и инициалы ответственного пользователя, номер городского рабочего телефона исполнителя (подразделения), дата постановки на учет и подпись лица, производившего учет.

исполнителя, фамилия лица, отпечатавшего (размножившего) документ, дата печатания документа.

Отпечатанные и подписанные документы вместе с черновиками передаются для регистрации сотруднику, ответственному за ведение делопроизводства в подразделении, осуществляющему их учет. Черновики и варианты уничтожаются этим сотрудником с отражением факта уничтожения в учетных формах.

Порядок обращения с документами ограниченного распространения с пометкой «Для служебного пользования» определен Временной инструкцией по делопроизводству в Вооруженных Силах Российской Федерации<sup>9</sup> (ВИД-2009).

47. Хранение МНИ должно осуществляться в условиях, исключающих их хищение, несанкционированное копирование или уничтожение содержащейся на них информации.

48. Подключение отчуждаемых МНИ из состава абонентского пункта ИТКС ОП «Интернет» к СВТ объектов информатизации подразделений академии **ЗАПРЕЩЕНО**.

При необходимости допускается перенос информации, полученной по каналам ИТКС ОП на МНИ, из состава объектов информатизации, которые определены в приказе начальника академии о вводе в эксплуатацию объекта информатизации подразделения. При этом на объекте информатизации должны быть приняты дополнительные меры по ЗИ:

назначено ответственное должностное лицо, уполномоченное на выполнение операций по переносу информации на МНИ из состава объекта информатизации;

перенос информации осуществляется в форматах данных, не содержащих в своем составе средств, предусматривающих автоматическую (автоматизированную) обработку данных при обращении к ним стандартными средствами операционных систем;

перенос (копирование) информации осуществляется через дополнительный учтенный и подготовленный для работы в составе средств объекта информатизации отчуждаемый МНИ на вспомогательном автономном СВТ с установленными и настроенными средствами ЗИ и антивирусной защиты;

использование одних и тех же МНИ в составе СВТ, подключаемых к сетям общего пользования и средствам из состава объекта информатизации, **запрещается**;

скопированная из ИТКС ОП информация хранится на МНИ вспомогательного СВТ **не менее месяца** после переноса на МНИ объекта информатизации.

49. По миновании надобности информация ограниченного распространения с пометкой «Для служебного пользования» с МНИ должна стираться установленным для этих носителей способом с использованием сертифицированных средств ЗИ (программных средств), реализующих функции стирания (маскирующего удаления) информации и отметкой в журнале учета стирания информации ([форма № 9](#))<sup>10</sup>.

50. По миновании надобности, с разрешения соответствующих начальников подразделений, МНИ, утратившие практическое значение и не имеющие исторической и иной ценности, подлежат уничтожению. МНИ уничтожаются комиссионно с составлением акта, при этом отрабатывается необходимый перечень документов для списания МНИ с учета академии как материальных ценностей<sup>11</sup>.

МНИ уничтожаются путем нанесения им неустранимого физического повреждения, исключающего возможность их использования и восстановления записанной на них информации. Выбор способа уничтожения МНИ должен осуществляться с учетом его физических свойств.

Уничтожение магнитных дисков осуществляется путем снятия с них магнитного покрытия механическим способом (с цилиндров и дисков) или плавлением цилиндров и дисков.

Сгораемые МНИ уничтожаются путем сжигания, расплавления, дробления, растворения или химического разложения, превращения в бесформенную массу или порошок. Допускается производить уничтожение (перевод в неработоспособное

<sup>9</sup> Утверждена решением Министра обороны Российской Федерации от 19 августа 2009 года № 205/2/588.

<sup>10</sup> Отметка в журнале учета стирания информации проставляется в случае, если производилось удаление информации ограниченного распространения с пометкой «Для служебного пользования».

<sup>11</sup> Определено приказом начальника академии от 13 мая 2014 года № 337.

состояние) МНИ с использованием сертифицированных специализированных устройств уничтожения информации.

## V. ОРГАНИЗАЦИЯ ПРИМЕНЕНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

51. Защита информационных ресурсов на объектах информатизации, обеспечение их конфиденциальности, целостности и доступности осуществляются с применением средств ЗИ.

Применяемые на объектах информатизации академии средства ЗИ должны иметь действующий сертификат соответствия по требованиям безопасности информации и соответствовать классам защищенности АС. Средства ЗИ, применяемые на объектах информатизации академии, должны предусматривать выполнение следующих основных функций:

защиту от несанкционированной начальной загрузки нештатной операционной системы;

защиту от НСД к информации;

защиту информации от воздействия компьютерных вирусов;

защиту информации при межсетевом взаимодействии;

сигнализацию о попытках НСД к защищаемым ресурсам объекта информатизации;

возможность настройки и удаленного управления средствами ЗИ администратором безопасности (ответственным за ЗИ), установленных на СВТ, подключенных (подключаемых) к локальным вычислительным сетям.

С учетом конкретных особенностей и условий эксплуатации (применения) СВТ в составе объектов информатизации могут применяться различные средства ЗИ, реализующие выполнение одной или нескольких указанных функций, либо комплексы ЗИ, обеспечивающие безопасность информации.

52. Комплекс работ по установке и настройке средств ЗИ на СВТ должен быть завершен до начала обработки защищаемой информации с их использованием.

Установка, настройка и управление режимами функционирования средств ЗИ осуществляются ответственными за ЗИ в подразделениях.

53. Настройка средств ЗИ объектов информатизации осуществляется в соответствии с эксплуатационной документацией на средства ЗИ и должна обеспечивать безопасность информации во всех режимах функционирования СВТ, предусмотренных инструкцией по ЗИ в подразделении.

Установка аппаратной части средств ЗИ проводится до установки программной части.

Установка программной части средств ЗИ проводится после установки средств общего, общесистемного и специального программного обеспечения с учетом следующих требований:

разделения дискового пространства на зоны<sup>12</sup> хранения информации исходя из функционального предназначения СВТ (АРМ пользователей, серверы различного назначения);

определения перечня системных (специальных) сервисов и параметров протоколов информационного взаимодействия, а также ресурса логических имен и адресов, необходимых для обеспечения функционирования программных средств в вычислительных сетях;

использования способов кодирования учетных записей пользователей и защищаемых ресурсов, обеспечивающих удобство управления средствами ЗИ, применяемыми на объекте информатизации;

обеспечения резервного копирования пользовательских данных (профилей настройки) и защищаемых ресурсов.

54. В ходе настройки средств ЗИ должны быть проведены<sup>13</sup>:

<sup>12</sup> Различают зоны для размещения файлов операционных систем, разделом для хранения промежуточных результатов и файлов подкачки, разделов с защищаемой информацией, специальные зоны для хранения служебной информации средств ЗИ и другие.

<sup>13</sup> Указанные требования распространяются также на комплексы телекоммуникационного оборудования, имеющие в своем составе средства ЗИ или реализующие отдельные функции ЗИ.

установка и настройка аппаратной части средств ЗИ, в том числе реквизитов учетных записей администраторов (пользователей и т.п.), политик безопасности, инициализация аппаратно-программных модулей доверенной загрузки и идентификаторов доступа;

установка и настройка программной части средств ЗИ, в том числе создание и настройка учетных записей пользователей на доступ к защищаемым ресурсам, создание списков контроля целостности, настройки подсистем регистрации и журналов безопасности;

настройка правил доступа к локальным или сетевым устройствам (станциям) печати;

настройка правил доступа к устройствам передачи данных, в том числе с использованием коммуникационных и почтовых программных средств;

настройка правил фильтрации потоков информации (при наличии межсетевых взаимодействий);

резервное копирование или создание образов МНИ с настроенным программным обеспечением и файлами защищаемых ресурсов;

генерация и установка паролей, а также доведение их до пользователей.

55. Предоставление пользователям доступа к защищаемым ресурсам объекта информатизации осуществляется после их аутентификации средствами ЗИ.

Прохождение процедуры аутентификации пользователей осуществляется с использованием идентификаторов доступа и паролей (кодов) или комбинации указанных способов.

При прохождении аутентификации на основе паролей, используются буквенно-цифровые символьные последовательности.

Параметры парольной защиты на объектах информатизации должны соответствовать основным требованиям, указанным в [форме № 25](#).

56. Учет идентификаторов доступа и паролей на вход в операционную систему пользователей (смарт-карты eToken, USB-ключи, электронно-ключевые носители Touch Memo и т.п.) на объектах информатизации осуществляется в отдельном разделе журнала учета МНИ ([форма № 10](#)).

Идентификаторы доступа выдаются пользователям под роспись в книге закрепления и выдачи идентификаторов доступа и паролей ([форма № 11](#)).

Хранение идентификаторов доступа осуществляется в сейфах или специальных шкафах (хранилищах) пользователей.

Пользователи, получившие идентификаторы доступа, несут персональную ответственность за их сохранность и использование.

57. Ввод и смена значений паролей пользователей производятся в соответствии с эксплуатационной документацией на средства ЗИ.

При проведении указанных работ должны обеспечиваться условия, исключающие компрометации вводимых значений паролей.

Периодичность смены кодов и паролей определяется графиком, утвержденным начальником объекта информатизации ([форма № 12](#)), в соответствии с основными требованиями к парольной защите на объектах информатизации ([форма № 25](#)), а также после окончания ремонтных (восстановительных) или других работ с привлечением специалистов организаций, имеющих соответствующие лицензии (в соответствии с заключенными государственными контрактами), в результате которых коды или пароли стали (могли стать) известны указанным лицам.

58. При компрометации паролей доступа, пользователи немедленно докладывают о случившемся начальнику объекта информатизации и ответственному за ЗИ и действуют по их указаниям.

Ответственный за ЗИ незамедлительно принимает меры к выводу из действия скомпрометированных (утраченных) паролей.

Обо всех фактах компрометации ответственным за ЗИ делается запись в журнале учета фактов НСД и воздействия компьютерных вирусов ([форма № 8](#)).

По фактам компрометации проводится служебное разбирательство (расследование) в установленном порядке.



59. Перечни защищаемых ресурсов готовятся путем анализа решаемых в интересах подразделений задач, состава и возможностей технических и программных средств объекта информатизации, организуемых баз данных, а также средств, обеспечивающих обмен информацией между объектами информатизации.

Составление перечней защищаемых ресурсов осуществляется до ввода объектов информатизации в эксплуатацию и уточняется ежегодно комиссией.

60. При разработке перечня защищаемых ресурсов ([форма № 6](#)) учитываются следующие категории учетных записей должностных лиц, имеющих права доступа к техническим и программным средствам и защищаемым ресурсам объекта информатизации:

пользователи;

администраторы баз данных (отдельные пользователи, с правами администрирования баз данных);

администраторы безопасности (ответственные за ЗИ);

администраторы аудита (штатный орган ОБИ).

Обработка информации, содержащейся в защищаемых ресурсах, осуществляется должностными лицами с использованием учетных записей, отнесенных к категориям пользователей.

Обработка информации в административных режимах запрещена.

Учетные записи администраторов баз данных и администраторов безопасности назначаются должностным лицам, ответственным за ЗИ на объектах информатизации.

Учетные записи администраторов аудита назначаются должностному лицу штатного органа ОБИ (офицеру службы ЗГТ).

61. Установка средств общего, общесистемного и специального программного обеспечения осуществляется администраторами безопасности (ответственными за ЗИ).

Создание и отнесение учетных записей к категориям пользователей, настройка правил разграничения доступа и режимов функционирования средств ЗИ проводятся ответственными за ЗИ на основании перечня защищаемых ресурсов и таблицей разграничения доступа ([формы №№ 6, 7](#)).

В ходе настройки ответственным за ЗИ выполняются следующие основные мероприятия<sup>14</sup>:

настройка безопасной начальной загрузки СВТ;

настройка связности СВТ в вычислительной сети объекта по физическим и логическим адресам;

создание учетных записей групп пользователей, характеризующихся определенными видами доступа к защищаемым ресурсам;

отключение уязвимых или неиспользуемых сетевых сервисов, не требующихся для выполнения задач, решаемых на СВТ;

настройка управления и обновления САВЗ;

настройка (определение) правил разграничения доступа к защищаемым ресурсам;

генерация и распределение паролей пользователей;

настройка средств контроля целостности средств ЗИ;

настройка правил выполнения операций ввода-вывода на печать и отчуждаемые МНИ;

настройка правил регистрации информации об обращениях пользователей к защищаемым ресурсам;

62. Подключение СВТ из состава объектов информатизации к ИТКС ОП, включая сеть Интернет, **запрещено**.

При необходимости, такое подключение производится в порядке, определенном приказом Министра обороны Российской Федерации 2012 года № 950дсп, только с использованием специально предназначенных для этого средств ЗИ, в том числе шифровальных (криптографических) средств, прошедших в установленном

<sup>14</sup> Перечень, объем и последовательность выполняемых работ могут отличаться от приведенных в настоящем пункте с учетом фактической структуры и состава технических и программных средств объекта информатизации.

законодательством Российской Федерации порядке сертификацию в ФСБ России и (или) получивших подтверждение соответствия ФСТЭК России.

## VI. ОРГАНИЗАЦИЯ РАБОТ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОТ ВОЗДЕЙСТВИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

63. Защита информации от воздействия компьютерных вирусов<sup>15</sup> (антивирусная защита) является неотъемлемой составной частью системы ЗИ, создаваемой на объектах информатизации.

Порядок осуществления антивирусной защиты определяется в отдельном разделе инструкции по ЗИ ([форма № 22](#)), в котором отражаются: обязанности должностных лиц по вопросам антивирусной защиты, порядок осуществления антивирусной защиты, порядок получения и применения САВЗ (обновлений БВС), периодичность проведения проверок СВТ на отсутствие компьютерных вирусов и проводимые мероприятия при их обнаружении.

64. Основным способом ЗИ от воздействия компьютерных вирусов является применение САВЗ.

Порядок применения САВЗ на СВТ должен включать следующие основные виды работ:

обязательную проверку на отсутствие компьютерных вирусов всей информации, поступающей (отправляемой) на МНИ, а также информации, содержащейся на МНИ объектов информатизации или получаемой (отправляемой) по каналам передачи данных; периодическую проверку<sup>16</sup> информации на МНИ.

Все программные средства перед вводом в эксплуатацию подлежат обязательной проверке на возможное наличие компьютерных вирусов. При обнаружении компьютерных вирусов применять указанное средство запрещается. О выявленном факте немедленно докладывается штатному органу ОБИ.

65. Поставка САВЗ в подразделения осуществляется штатным органом ОБИ.

Поставка обновлений БВС САВЗ осуществляется еженедельно.

После поступления копий файлов (архивов с файлами) САВЗ и обновлений БВС на объекты информатизации проводится подсчет контрольных сумм содержащихся на них файлов и их сравнение со значениями контрольных сумм, передаваемых вместе с копиями файлов (архивов с файлами) САВЗ и обновлениями БВС.

В случае несоответствия контрольных сумм использование установочного комплекта САВЗ и обновлений БВС запрещается.

Передача САВЗ и обновлений БВС, полученных в службе ЗГТ академии, в организации, не относящиеся к Минобороны России, а также использование на СВТ личного пользования запрещается.

66. САВЗ и обновления БВС подлежат установке на все СВТ объектов информатизации.

Установка САВЗ проводится в соответствии с эксплуатационной документацией на них ответственными за ЗИ в течение **пяти рабочих дней** со дня получения САВЗ, а обновления БВС – в течение **двух рабочих дней** со дня получения обновлений БВС.

67. При обнаружении компьютерных вирусов (возникновении подозрения на их наличие) пользователь обязан немедленно прекратить обработку информации, доложить ответственному за ЗИ и в соответствии с его указаниями выполнить поиск и удаление компьютерных вирусов.

---

<sup>15</sup> Здесь и далее в тексте под компьютерными вирусами понимаются не только программы, способные создавать свои копии (необязательно совпадающие с оригиналом), но и другие программные средства скрытого информационного воздействия и вредоносные программы (сетевые черви, логические бомбы, троянские и шпионские программы).

<sup>16</sup> Периодичность проверки устанавливается начальником объекта информатизации, исходя из следующего:

проверка съемных МНИ – каждый раз при подключении к СВТ;

проверка встроенных МНИ (ЖМД) – не реже одного раза в неделю.

Также полная проверка встроенных МНИ (ЖМД) проводится после обновления БВС САВЗ.

САВЗ, установленные на СВТ объектов информатизации позволяют настроить периодичность вышеуказанных проверок в автоматическом режиме без участия пользователей.

Факты воздействия компьютерных вирусов учитываются ответственным за ЗИ в журнале учета фактов НСД и воздействия компьютерных вирусов ([форма № 8](#)).

В случаях, когда удаление отдельных типов компьютерных вирусов или фрагментов их кода невозможно без стирания (удаления) файла, в котором они обнаружены, осуществляется стирание (удаление) файла.

68. При воздействии компьютерных вирусов на СВТ, функционирующее в составе вычислительной сети, производится ее физическое отключение от сети. Проверка средств информационного и программного обеспечения на наличие компьютерных вирусов в этом случае осуществляется на всех СВТ (рабочих станциях, серверах и т.п.), входящих в состав вычислительной сети объекта информатизации.

69. В случае выявления информации (файлов, наборов данных), подозрительной на наличие компьютерных вирусов, которые не обнаруживаются имеющимися САВЗ, ответственным за ЗИ докладывается об этом начальнику объекта информатизации и в штатный орган ОБИ рапортом.

Указанная информация (файлы, наборы данных) передается в штатный орган ОБИ. Перед передачей на МНИ с такой информацией наносится маркировка: **«Осторожно! Компьютерные вирусы!»**.

Обработка информации на СВТ, на которых обнаружены указанные файлы, приостанавливается до принятия совместного решения начальника объекта информатизации и начальника службы – помощника начальника академии по ЗГТ.

70. По всем фактам обнаружения компьютерных вирусов ответственным за ЗИ совместно со штатным органом ОБИ должны проводиться анализ причин, повлекших возможность проникновения (определен источник) и воздействия компьютерных вирусов на объект информатизации, и оценка последствий этого воздействия.

## VII. КОНТРОЛЬ ОРГАНИЗАЦИИ И СОСТОЯНИЯ РАБОТЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ

71. Контроль организации и состояния работы по ЗИ осуществляется в целях получения ее объективной оценки, поддержания системы ЗИ в подразделениях на требуемом уровне и при необходимости своевременного принятия соответствующих мер по предупреждению возможных нарушений и повышению безопасности информации.

Контроль организации и состояния работы по ЗИ осуществляется:

начальником объекта информатизации и ответственным за ЗИ – на объекте информатизации подразделения не реже 1 раза в месяц (результаты отражаются в ежемесячном рапорте о состоянии ЗИ);

службой ЗГТ – во всех подразделениях согласно планам проверок.

72. Ежемесячно к **30 числу** начальники подразделений докладывают рапортом о состоянии ЗИ и выполненных мероприятиях по ЗИ на объектах информатизации подразделения на имя заместителя начальника академии через службу ЗГТ академии ([форма № 21](#)).

73. Допуск должностных лиц службы ЗГТ академии, прибывших в подразделение для проверки объектов информатизации, осуществляется в установленном порядке<sup>17</sup>.

Проверки проводятся в присутствии ответственных должностных лиц объекта информатизации и (или) лиц, их замещающих.

74. Контроль правильности использования защищаемых ресурсов на объекте информатизации осуществляется с использованием средств ЗИ и (или) средств регистрации событий операционных систем на каждом СВТ<sup>18</sup> (системные журналы операционных систем, журналы средств ЗИ, log-файлы и т.д.).

Регистрационная информация анализируется ответственным за ЗИ не реже одного раза в месяц, а также в случае обнаружения фактов НСД или действий пользователей,

<sup>17</sup> Определено ежегодным планом мероприятий ЗГТ академии, а также по отдельному плану внезапных проверок состояния ЗГТ в подразделениях академии.

<sup>18</sup> Если СВТ подключены к вычислительной сети, в которой предусмотрено АРМ ответственного за ЗИ, журналы регистрации информации об обращениях к защищаемым ресурсам операционной системы и средства ЗИ разрешается вести только на данном компьютере.

нарушающих правила разграничения доступа (попыток НСД). Порядок проведения анализа и конкретные сроки определяются в инструкции по ЗИ ([форма № 22](#)) на объекте информатизации.

В случае выявления зарегистрированных фактов обращения пользователей с нарушением назначенных им прав или привилегий, предоставленных администратором безопасности (при выявлении признаков (предпосылок) НСД к информации), проводится разбирательство.

Сведения о факте (код сообщения, дата, время и наименование учетной записи), результаты анализа причин и принятые решения записываются в журнал учета фактов НСД и воздействия компьютерных вирусов ([форма № 8](#)) с докладом начальнику подразделения, эксплуатирующего объект информатизации и уведомлением органа ОБИ службы ЗГТ.

75. При проведении проверок состояния работы по ЗИ допускается использование средств контроля эффективности ЗИ.

**НАЧАЛЬНИК СЛУЖБЫ – ПОМОЩНИК НАЧАЛЬНИКА  
АКАДЕМИИ ПО ЗГТ  
полковник**

**О.Варсегов**

**КЛАССЫ**  
защищенности от НСД АС (объектов информатизации) академии

Таблица 1

Уровень конфиденциальности обрабатываемой информации	Класс защищенности АС (объекта информатизации)		
	Один пользователь, допущенный ко всей информации	От двух и больше пользователей	
		Одинаковые права доступа (полномочия) к информации	Различные права доступа (полномочия) к информации
1	2	3	4
Информация ограниченного распространения с пометкой «Для служебного пользования»	1Г		
Служебная несекретная информация	3Б	2Б	1Д

Требования к подсистемам классов защищенности от НСД к информации:

Обозначения:

" – " - нет требований к данному классу;

" + " - есть требования к данному классу.

Таблица 2

Подсистемы и требования	Классы			
	1Г	1Д	2Б	3Б
<b>1. Подсистема управления доступом.</b>				
Идентификация, проверка подлинности и контроль доступа субъектов:				
в систему	+	+	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	+	–	–	+
к программам	+	–	–	–
к томам, каталогам, файлам, записям, полям записей	+	–	–	–
<b>2. Подсистема регистрации и учета.</b>				
Регистрация и учет:				
входа (выхода) субъектов доступа в (из) систему (узел сети)	+	+	+	+
выдачи печатных (графических) выходных документов	+	–	–	–
запуска (завершения) программ и процессов (заданий, задач)	+	–	–	–
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	+	–	–	–
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	+	–	–	–
учет носителей информации	+	+	+	+
очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	+	–	–	–
<b>3. Подсистема обеспечения целостности</b>				
обеспечение целостности программных средств и обрабатываемой информации	+	+	+	+
физическая охрана средств вычислительной техники и носителей информации	+	+	+	+
наличие администратора (ответственного за ЗИ)	+	+	+	+
периодическое тестирование СЗИ НСД	+	+	+	+
наличие средств восстановления СЗИ НСД	+	+	+	+
использование сертифицированных средств защиты информации	+	+	+	+

УТВЕРЖДАЮ  
Заместитель начальника академии  
полковник  
С.Чистяков  
« \_\_\_\_ » марта 2015 года

**АКТ**  
**классификации (установки уровня защищенности) объекта информатизации**  
**000 кафедры Военно-космической академии имени А.Ф.Можайского**

« \_\_\_\_ » марта 2015 года

г. Санкт-Петербург

Комиссия, назначенная приказом начальника академии от 28 апреля 2015 года № 14дсп в составе: председателя комиссии начальника 000 кафедры полковника ИВАНОВА И.И., членов комиссии: начальника узла связи академии майора ДУБОВА В.В., офицера по обеспечению безопасности информации и режима секретности службы защиты государственной тайны (ЗГТ) академии старшего лейтенанта БЕЛЯКОВА М.И., ответственного за защиту информации (ЗИ) капитана ЖАБУНОВА А.А. и ответственного за эксплуатацию программных и технических средств на объекте информатизации лейтенанта ЗАЗУЛЯ О.О., рассмотрела исходные данные объекта информатизации 000 кафедры и установила:

1. Характер обрабатываемой информации (ограниченного распространения с пометкой «Для служебного пользования» или служебная несекретная).

2. Условия эксплуатации (одно- или многопользовательский режим обработки информации с равными или различными правами доступа к информации).

В соответствии с Руководством по защите информации от несанкционированного доступа в Вооруженных Силах Российской Федерации, утвержденного приказом Министра обороны Российской Федерации 2013 года № 011 и Инструкцией по организации в Вооруженных Силах Российской Федерации защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, обрабатываемой в государственных информационных системах и информационных системах персональных данных, утвержденной приказом Министра обороны Российской Федерации 2014 года № 925дсп комиссия решила:

установить объекту информатизации 000 кафедры (или отдельным СВТ) класс защищенности (уровень защищенности) – 1Г<sup>19</sup>.

*Если на объекте информатизации только на некоторых ПЭВМ предполагается обработка информации «Для служебного пользования», то в акте указывается:*

установить АРМ № 1-15 00 кафедры класс защищенности (уровень защищенности) – 1Д<sup>20</sup>, для АРМ № 16-18 – 1Г<sup>21</sup>.

Председатель комиссии:

полковник

И.Иванов

Члены комиссии:

майор

В.Дубов

капитан

А.Жабунув

старший лейтенант

М.Беляков

лейтенант

О.Зазуля

<sup>19</sup> Класс защищенности от НСД определяется методом соотношения условий обработки информации на объекте информатизации (отдельных АРМ), указанных в п.п. №№ 1-2 настоящего акта и таблице 1 формы № 1 настоящих Методических рекомендаций... Для объектов информатизации, на которых обрабатывается информация ограниченного распространения с пометкой «Для служебного пользования», класс защищенности должен быть не ниже класса защищенности 1Г.

<sup>20</sup> На данных АРМ обрабатывается служебная несекретная информация.

<sup>21</sup> На данных АРМ обрабатывается информация ограниченного распространения с пометкой «Для служебного пользования».

**УТВЕРЖДАЮ**  
Заместитель начальника академии  
полковник  
С.Чистяков  
«\_\_» марта 2015 года

**АКТ**  
**ввода в эксплуатацию средств общего программного обеспечения и средств ЗИ**  
**на объекте информатизации 000 кафедры Военно-космической академии**  
**имени А.Ф.Можайского**

«\_\_» марта 2015 года

г. Санкт-Петербург

Комиссия, назначенная приказом начальника академии от 28 апреля 2015 года № 14дсп в составе: председателя комиссии начальника 000 кафедры полковника ИВАНОВА И.И., членов комиссии: начальника узла связи академии майора ДУБОВА В.В., офицера по обеспечению безопасности информации и режима секретности службы защиты государственной тайны (ЗГТ) академии старшего лейтенанта БЕЛЯКОВА М.И., ответственного за защиту информации (ЗИ) капитана ЖАБУНОВА А.А. и ответственного за эксплуатацию программных и технических средств на объекте информатизации лейтенанта ЗАЗУЛЯ О.О., провела проверку полноты и качества установки, настройки средств общего программного обеспечения и средств защиты информации на объекте информатизации 000 кафедры и установила:

1. На средствах ВТ объекта информатизации установлено следующее общее программное обеспечение и средства ЗИ:

№ п/п	Наименование общего программного обеспечения и средства ЗИ <sup>1</sup>	Выполняемые функции	Контрольная сумма <sup>2</sup>
1.	Windows 7 Professional	Автоматизация повседневной деятельности должностных лиц кафедры	-
2.	Secret Net 7.2	Средство защиты информации от несанкционированного доступа к информации, обрабатываемой на АРМ объекта информатизации кафедры	e80aed782fe28ec52dd943e7fe5be291
3.	Dr.Web Security Space version 9.1	Средство антивирусной защиты	4f5b6bce700148f830d8fab824194ab0
4.	Kaspersky Endpoint Security 8 для Windows	Средство антивирусной защиты	04332b7b7c90d411530229cc8db379af

2. Общее и специальное программное обеспечение, установленное на средствах ВТ объекта информатизации входит в Перечень средств программного обеспечения, разрешенных к применению на АРМ должностных лиц Минобороны России, утвержденный приказом Министра обороны Российской Федерации от 2012 года № 3799дсп.

**Вывод:** средства общего программного обеспечения и средства ЗИ установлены и настроены на средствах ВТ объекта информатизации 000 кафедры в соответствии с требованиями руководящих документов в области защиты информации от НСД и эксплуатационной документацией.

Председатель комиссии:

полковник

И.Иванов

Члены комиссии:

майор

В.Дубов

капитан

А.Жабунув

старший лейтенант

М.Беляков

лейтенант

О.Зазуля

<sup>1</sup> В данной графе указывается наименование общего программного обеспечения (MS BC 3.0, Linux, Windows XP/Vista/7/8/Server 2003(8) и т.п.), специального программного обеспечения (программы работы с графикой, текстовыми документами, справочники и т.п.) и средств ЗИ и САВЗ (Secret Net 5.0, 6.0, 7.2; Страж NT, АПМДЗ «Соболь», АПМДЗ «Центурион», Dr. Web или Kaspersky и т.п.)

<sup>2</sup> В данной графе указываются контрольные суммы файлов, указанные в паспортах (паспортах-формулярах) или на лицензионных дисках на соответствующее программное (программно-аппаратное) изделие. Если контрольные суммы отсутствуют, то ставится прочерк.

УТВЕРЖДАЮ  
Заместитель начальника академии  
полковник  
С.Чистяков  
« \_\_\_\_ » марта 2015 года

**АКТ  
готовности системы защиты информации объекта информатизации 000 кафедры  
Военно-космической академии имени А.Ф.Можайского**

« \_\_\_\_ » марта 2015 года

г. Санкт-Петербург

Комиссия, назначенная приказом начальника академии от 28 апреля 2015 года № 14дсп в составе: председателя комиссии начальника 000 кафедры полковника ИВАНОВА И.И., членов комиссии: начальника узла связи академии майора ДУБОВА В.В., офицера по обеспечению безопасности информации и режима секретности службы защиты государственной тайны (ЗГТ) академии старшего лейтенанта БЕЛЯКОВА М.И., ответственного за защиту информации (ЗИ) капитана ЖАБУНОВА А.А. и ответственного за эксплуатацию программных и технических средств на объекте информатизации лейтенанта ЗАЗУЛЯ О.О., провела проверку готовности системы ЗИ на объекте информатизации 000 кафедры и установила:

1. Состав технических средств объекта информатизации:

№ п/п	Наименование и состав основного оборудования	Заводской (серийный) номер
1.	2.	3.
<b>3 этаж учебного корпуса № 1, помещение № 514</b>		
АРМ № 1		
1.	Системный блок Aquarius Pro P30 S61	MLGK875JNBKJ
2.	Клавиатура Logitech MK 120-USB	3KM2HN4M5K
3.	Манипулятор «мышь» оптическая Logitech M-U0026	24MM2K56M43
4.	Монитор АОС E960Srda	MLLKIOOLFKI67
5.	Источник бесперебойного питания APC BK500-RS	4B1326P49851
6.	Сетевой фильтр Defender ESS	б/н
<b>3 этаж учебного корпуса № 1, помещение № 517</b>		
АРМ № 2		
7.	Системный блок Aquarius Pro P30 S61	2140416629133-0111
8.	Клавиатура Logitech MK 120-USB	902238118928104
9.	Манипулятор «мышь» оптическая Logitech M-U0026	7K4971
10.	Монитор АОС E960Srda	FMJE1HA046953
11.	Источник бесперебойного питания APC BK500-RS	4B1326P44736
12.	Сетевой фильтр Defender ESS	б/н
13.	Принтер Xerox Phaser 3160N	3960454781

2. Несанкционированных подключений к ИТКС, в том числе ИТКС ОП «Интернет», не выявлено.<sup>1</sup>

3. Время работы пользователей – согласно регламенту служебного (рабочего) времени.

4. Пользователям доступны только ресурсы в соответствии с таблицей разграничения доступа.

5. В целях выполнения мероприятий по защите информации выполнены следующие мероприятия:

система разграничения доступа к защищаемым ресурсам настроена в соответствии с таблицей разграничения с помощью средств ЗИ Secret Net 7.2 и (или) АПМДЗ «Центурион»;<sup>1</sup>

<sup>1</sup> Комиссия в обязательном порядке проверяет наличие подключений к ИТКС. В случае, если средства(о) ВТ объекта информатизации установленным порядком подключены(о) к какой-либо сети (ЛВС подразделения или внутренняя сеть академии «Электронный ВУЗ»), то это указывается в данном пункте, например: «АРМ №№ 1-4 установленным порядком подключены к ИТКС академии «Электронный ВУЗ» или ЛВС 00 кафедры», а после указывается «Несанкционированных подключений к другим ИТКС, в том числе ИТКС ОП «Интернет» не выявлено». В случае выявления несанкционированных подключений к ИТКС, в том числе и к ИТКС ОП «Интернет», осуществляется доклад начальнику службы ЗГТ академии, после чего проводится разбирательство по данному факту.



установлен пароль на вход в меню настроек базовой системы ввода-вывода (BIOS);<sup>2</sup>

установлены средства антивирусной защиты Kaspersky Security Endpoint 8 для Windows (Doctor Web 5.0 (6.0) или Kaspersky for Windows Workstation 6.0) (если в состав объекта информатизации входят отдельные АРМ, на которых установлены UNIX-подобные системы, то на них в обязательном порядке ставится САВЗ Kaspersky Endpoint Security 8 for Linux или Dr.Web для файловых серверов UNIX, или рабочих станций Dr.Web Enterprise Suite Special Edition (agent) ver. 6.0);

на средствах ВТ объекта информатизации проведено отключение функции автозапуска с внешних машинных носителей информации;

проверка функционирования средств ЗИ от НСД и САВЗ, а также параметров их настроек проведена в соответствии с инструкциями, поставляемыми в комплекте с этими средствами и таблицей разграничения доступа к защищаемым ресурсам объекта информатизации соответственно;<sup>3</sup>

проверка исправности технических средств охраны помещения(й), в котором размещен(ы) технические средства (СВТ) объекта информатизации, проведена методом вскрытия помещений и окон при работающей сигнализации<sup>4</sup>.

**Вывод:** организационные и практические мероприятия по ЗИ, исправное состояние и настройка параметров средств ЗИ на объекте информатизации 00 кафедры позволяют производить работы по обработке: на АРМ №№ 1-15 – служебной несекретной информации; на АРМ №№ 16-18 – информации ограниченного распространения с пометкой «Для служебного пользования», соответствующие классам защищенности, определенными в акте классификации объекта (уч. № 00 от 00.00.2015 года).

Председатель комиссии:

полковник

И.Иванов

Члены комиссии:

майор

В.Дубов

капитан

А.Жабунев

старший лейтенант

М.Беляков

лейтенант

О.Зазуля

<sup>1</sup> В данном пункте указываются все сертифицированные по требованиям безопасности информации программно-аппаратные, программные и(или) аппаратные средства ЗИ, с помощью которых организовано разграничение доступа к защищаемым ресурсам.

<sup>2</sup> Если на средствах(е) ВТ объекта информатизации подразделения установлен и настроен аппаратно-программный модуль доверенной загрузки (АПМДЗ) («Соболь», «Страж NT», «Центурион» и т. п.) и настроен пароль на вход, то пароль администратора на изменение параметров загрузки в меню базовой системы ввода-вывода (BIOS) допускается не устанавливать.

<sup>3</sup> На каждое поставляемое средство имеется документация по проверке действий функций определенного средства ЗИ. При проверке настроек и защитных функций средства ЗИ комиссия руководствуется данной документацией.

<sup>4</sup> Данный абзац указывается в случае, если помещения, в которых размещены технические средства, оборудованы средствами охраны.

УТВЕРЖДАЮ  
Заместитель начальника академии  
полковник

С.Чистяков

« \_\_\_\_ » марта 2015 года

**АКТ**  
**проверки функционирования средств ЗИ и системы предупреждения о НСД**  
**к техническим средствам объекта информатизации 000 кафедры**  
**Военно-космической академии имени А.Ф.Можайского**

« \_\_\_\_ » марта 2015 года

г. Санкт-Петербург

Комиссия, назначенная приказом начальника академии от 28 апреля 2015 года № 14дсп в составе: председателя комиссии начальника 000 кафедры полковника ИВАНОВА И.И., членов комиссии: начальника узла связи академии майора ДУБОВА В.В., офицера по обеспечению безопасности информации и режима секретности службы защиты государственной тайны (ЗГТ) академии старшего лейтенанта БЕЛЯКОВА М.И., ответственного за защиту информации (ЗИ) капитана ЖАБУНОВА А.А. и ответственного за эксплуатацию программных и технических средств на объекте информатизации лейтенанта ЗАЗУЛЯ О.О., провела проверку функционирования средств ЗИ системы предупреждения о несанкционированном доступе (НСД) к техническим средствам объекта информатизации 000 кафедры и установила:

1. Несанкционированных подключений к ИТКС, в том числе ИТКС ОП «Интернет», не выявлено.<sup>1</sup>

2. В целях выполнения мероприятий по защите информации выполнены следующие мероприятия: разграничение доступа на объекте информатизации организовано с помощью средств ЗИ Secret Net 7.2;<sup>2</sup>

система разграничения доступа к защищаемым ресурсам настроена в соответствии с таблицей разграничения доступа к защищаемым ресурсам объекта информатизации;

установлен пароль на вход в меню настроек базовой системы ввода-вывода (BIOS);<sup>3</sup>

установлены средства антивирусной защиты Kaspersky Endpoint Security 8 для Windows (Doctor Web 5.0 (6.0) или Kaspersky for Windows Workstation 6.0) (если в состав объекта информатизации входят отдельные АРМ, на которых установлены UNIX-подобные системы, то на них в обязательном порядке ставится САВЗ Kaspersky Endpoint Security 8 for Linux или Dr.Web для файловых серверов UNIX, или рабочих станций Dr.Web Enterprise Suite Special Edition (agent) ver. 6.0);

на средствах ВТ объекта информатизации функция автозапуска с внешних машинных носителей информации отключена;

идентификаторы доступа и пароли для доступа к защищаемым ресурсам объекта информатизации выдаются под роспись в Книге закрепления и выдачи идентификаторов доступа и паролей.

Проверка функционирования средств ЗИ от НСД и САВЗ, а также параметров их настроек проводилась в соответствии с инструкциями, поставляемыми в комплекте с этими средствами и таблицей разграничения доступа к защищаемым ресурсам объекта информатизации соответственно.<sup>4</sup>

5. Проверка исправности технических средств охраны помещения(й), в котором размещен объект информатизации, проведена методом вскрытия помещений и окон при работающей сигнализации<sup>5</sup>.

---

1 Комиссия в обязательном порядке проверяет наличие подключений к ИТКС. В случае, если средства(о) ВТ объекта информатизации установленным порядком подключены(о) к какой-либо сети (СЭД, ОС СПД, ЗС СПД, «Тонкий клиент», внутренняя сеть академии «Электронный ВУЗ», АП ИТКС «Интернет» или др.), то это указывается в данном пункте, например: «АРМ №№ 1-4 установленным порядком подключены к ИТКС академии «Электронный ВУЗ» или ИТКС ОП «Интернет», а после указывается «Несанкционированных подключений к другим ИТКС, в том числе ИТКС ОП «Интернет» не выявлено». В случае выявления несанкционированных подключений к ИТКС, в том числе и к ИТКС ОП «Интернет», осуществляется доклад заместителю начальника академии через службу ЗГТ академии, после чего проводится разбирательство по данному факту.

2 В данном пункте указываются все сертифицированные по требованиям безопасности информации программно-аппаратные, программные и(или) аппаратные средства ЗИ, используемые на объекте информатизации. Средства ЗИ, не сертифицированные по требованиям безопасности, использовать на средствах ВТ категорически запрещено.

3 Если на средствах(е) ВТ объекта информатизации подразделения установлен и настроен аппаратно-программный модуль доверенной загрузки (АПМДЗ) («Соболь», «Страж NT», «Центурион» и т. п.) и настроен пароль на вход, то пароль администратора на изменение параметров загрузки в меню базовой системы ввода-вывода (BIOS) допускается не устанавливать.

4 На каждое поставляемое средство имеется документация по проверке действий функций системы определенного средства ЗИ. При проверке настроек и защитных функций средства ЗИ комиссия руководствуется данной документацией.

5 Данный абзац указывается в случае, если помещения, в которых размещены технические средства, оборудованы средствами охраны.

**Вывод:** организационные и практические мероприятия по ЗИ, исправное состояние и настройка параметров средств ЗИ на объекте информатизации 00 кафедры позволяют производить работы по обработке: на АРМ №№ 1-15 – служебной несекретной информации; на АРМ №№ 16-18 – информации ограниченного распространения с пометкой «Для служебного пользования», соответствующие классам защищенности, определенными в акте классификации объекта (уч. № 00 от 00.00.2015 года).

Председатель комиссии:

полковник

И.Иванов

Члены комиссии:

майор

В.Дубов

капитан

А.Жабунов

старший лейтенант

М.Беляков

лейтенант

О.Зазуля

УТВЕРЖДАЮ  
Заместитель начальника академии  
полковник  
С.Чистяков  
« \_\_\_\_ » марта 2015 года

ПЕРЕЧЕНЬ  
защищаемых ресурсов объекта информатизации 000 кафедры академии

№ п/п	Порядковый номер АРМ/номер МНИ по журналу учета	Наименование защищаемого ресурса			Мандатная		Разрешенные виды доступа					К ресурсу допущены
		полное	условное	каталог	метка	категория	R	W	X	M	F	
1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.
<b>Пример для локальных компьютеров, не подключенных к какой-либо локальной вычислительной сети</b>												
1.	АРМ № 1/уч. №	Логический диск (C:/)	C:/	Programm Files	НС	Администраторы	+	+	+	+	+	Ответственный за ЗИ (администратор)
				Programm Data								
				Windows								
				MSOCache								
				Пользователи (или users)/Петров	ДСП	Пользователи	+	+	+	+	+	л-т Петров В.В. Ответственный за ЗИ (администратор)
				Пользователи (или users)/Иванов	ДСП							п/п-к Иванов И.И. Ответственный за ЗИ (администратор)
				Пользователи (или users)/Общие	НС							п/п-к Иванов И.И., л-т Петров В.В., Ответственный за ЗИ (администратор)
		Логический диск (D:/)	D:/	Рабочие материалы/Иванов	ДСП							п/п-к Иванов И.И., Ответственный за ЗИ (администратор)

№ п/п	Порядковый номер АРМ/номер МНИ по журналу учета	Наименование защищаемого ресурса			Мандатная		Разрешенные виды доступа					К ресурсу допущены			
		полное	условное	каталог	метка	категория	R	W	X	M	F				
1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.			
				Рабочие материалы/Петров	ДСП		+	+	+	+	+	л-т Петров В.В. Ответственный за ЗИ (администратор)			
				Рабочие материалы/Рук.доки	ДСП		+	–	–	–	+	п/п-к Иванов И.И., л-т Петров В.В., Ответственный за ЗИ (администратор)			
		DVD RW дисковод (H:/)	H:/	–	–		+	+	+	+	+	п/п-к Иванов И.И., л-т Петров В.В., Ответственный за ЗИ (администратор)			
		Принтер Xerox Workcentre 3210										п/п-к Иванов И.И., л-т Петров В.В., Ответственный за ЗИ (администратор)			
Пример для компьютерных классов подразделения															
2.	Компьютерный класс кафедры АРМ № 2/уч. № АРМ № 3/ уч. № АРМ № 4/ уч. № АРМ № 5/ уч. № АРМ № 6/ уч. № АРМ № 7/ уч. № АРМ № 8/ уч. № АРМ № 9/ уч. № АРМ № 10/ уч. №	Логический диск (C:/)	C:/	Programm Files	НС	Администраторы	+	+	+	+	+	Ответственный за ЗИ (администратор)			
				Programm Data			+	+	+	+	+				
				Windows			+	+	+	+	+				
				MSOCache			+	+	+	+	+				
				Пользователи (или users)/Слушатели		Пользователи	+	+	+	+	+	Слушатели Ответственный за ЗИ (администратор)			
				Пользователи (или users)/Курсанты			+	+	+	+	+		Курсанты Ответственный за ЗИ (администратор)		
				Пользователи (или users)/Преподаватели			+	+	+	+	+			Преподаватели Ответственный за ЗИ (администратор)	
				Пользователи (или users)/Адьюнкты			+	+	+	+	+				Адьюнкты Ответственный за ЗИ (администратор)
				Пользователи (или users)/Общие			+	+	+	+	+				

№ п/п	Порядковый номер АРМ/номер МНИ по журналу учета	Наименование защищаемого ресурса			Мандатная		Разрешенные виды доступа					К ресурсу допущены
		полное	условное	каталог	метка	категория	R	W	X	M	F	
1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.
												Ответственный за ЗИ (администратор)
		Логический диск (D:/)	D:/	Пользователи (или users)/Слушатели	НС	Пользова- тели	+	+	+	+	+	Слушатели Ответственный за ЗИ (администратор)
				Пользователи (или users)/Курсанты			+	+	+	+	+	Курсанты Ответственный за ЗИ (администратор)
				Пользователи (или users)/Преподаватели			+	+	+	+	+	Преподаватели Ответственный за ЗИ (администратор)
				Пользователи (или users)/Адъюнкты			+	+	+	+	+	Адъюнкты Ответственный за ЗИ (администратор)
				Пользователи (или users)/Общие			+	+	+	+	+	Слушатели Курсанты Преподаватели Адъюнкты Ответственный за ЗИ (администратор)
		DVD RW дисковод (H:/)	H:/	–	–		+	+	+	+	+	Слушатели Курсанты Преподаватели Адъюнкты Ответственный за ЗИ (администратор)
		Принтер HP Laser Jet 0000 mfp										Слушатели Курсанты Преподаватели Адъюнкты Ответственный за ЗИ (администратор)
Пример для компьютеров, подключенных к локальной вычислительной сети подразделения (либо к сети академии «Электронный ВУЗ»)												
3.	АРМ № 11/уч. №	Логический диск (C:/)	C:/	Programm Files	НС	Админист- раторы	+	+	+	+	+	Ответственный за ЗИ (администратор)
				Programm Data			+	+	+	+	+	

№ п/п	Порядковый номер АРМ/номер МНИ по журналу учета	Наименование защищаемого ресурса			Мандатная		Разрешенные виды доступа					К ресурсу допущены
		полное	условное	каталог	метка	категория	R	W	X	M	F	
1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.
				Windows			+	+	+	+	+	
				MSOCache			+	+	+	+	+	
				Буйликов	НС	Пользова- тели	+	+	+	+	+	Буйликов Ответственный за ЗИ (администратор)
				Лысенко			+	+	+	+	+	Лысенко Ответственный за ЗИ (администратор)
				Беляков	ДСП		+	+	+	+	+	Беляков Ответственный за ЗИ (администратор)
				Общая сетевая	НС		+	+	+	+	+	Буйликов Беляков Лысенко Ответственный за ЗИ (администратор)
		Логический диск (D:/)	D:/	Буйликов	НС		+	+	+	+	+	Буйликов Ответственный за ЗИ (администратор)
				Лысенко			+	+	+	+	+	Лысенко Ответственный за ЗИ (администратор)
				Беляков	ДСП		+	+	+	+	+	Беляков Ответственный за ЗИ (администратор)
				Материалы для занятий	НС		+	+	+	+	+	Буйликов Беляков Лысенко Ответственный за ЗИ (администратор)
		Сетевой диск (V:/)	V:/	Рапорта	НС		+	+	+	+	+	Буйликов Беляков Лысенко Ответственный за ЗИ (администратор)
				Рук.доки			+	+	+	+	+	
				Программы			+	+	—	—	+	
				Приказы НВКА			+	+	—	—	+	
		DVD RW	H:/	—	—		+	+	+	+	+	

№ п/п	Порядковый номер АРМ/номер МНИ по журналу учета	Наименование защищаемого ресурса			Мандатная		Разрешенные виды доступа					К ресурсу допущены
		полное	условное	каталог	метка	категория	R	W	X	M	F	
1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.
		дисковод (H:/)										
		Принтер HP Laser Jet 0000 mfp										Буйликов Беляков Лысенко Ответственный за ЗИ (администратор)
	Сетевой принтер/ уч. №	Принтер Xerox Workcentre 5220										

Председатель комиссии:

полковник

И.Иванов

Члены комиссии:

майор

В.Дубов

капитан

А.Жабунев

старший лейтенант

М.Беляков

лейтенант

О.Зазуля

**Примечания:** 1. Виды Доступа: R – чтение, W – запись, X – чтение и исполнение, M – изменение, F – поиск; «+» – вид доступа разрешен, «-» – вид доступа запрещен.  
2. Структура каталогов защищаемых ресурсов определяется в произвольной форме пользователями совместно с ответственными за ЗИ на объектах.



ТАБЛИЦА РАЗГРАНИЧЕНИЯ ДОСТУПА  
к защищаемым ресурсам \_\_\_\_\_  
(наименование объекта информатизации, воинской части)

№ п/п	Воинское звание, фамилия, инициалы, логическое имя	Наименование защищаемого ресурса														
		ARM № 1					ARM № 2-10					ARM № 11				
		А:	С:	D:	Е:	принтер	А:	С:	D:	Е:	принтер	А:	С:	D:	Е:	принтер
1	Полковник Иванов И.И. ivanov	Полн.	Полн.	Полн.	Полн.	+	-	-	-	-	-	-	-	-	-	-
2	Подполковник Петров П.П. petrov	R, X	R, X	R, X	R, X	-	-	-	-	-	-	-	-	-	-	-
3	Подполковник Сидоров С.С. sidorov	R, W	R	R, F	R, F	+	R	R	R	R	-	-	-	-	-	-
4	Буйликов Builikov	-	-	-	-	-	Полн.	Полн.	Полн.	Полн.	Полн.					Полн.
5	Беляков Belaykov	-	-	-	-	-	R	R	R	R	-	Полн.	Полн.	Полн.	Полн.	R, W, M
6	Лысенко Lisenko	-	-	-	-	-	-	-	-	-	-	Полн.	Полн.	Полн.	Полн.	R

Начальник 000 кафедры (начальник объекта информатизации)  
(должность)

ПОЛКОВНИК \_\_\_\_\_ И.Иванов  
(воинское звание, подпись, инициал имени, фамилия)

« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

**Примечания:** 1. Виды Доступа: R – чтение, W – запись, X – чтение и исполнение, M – изменение, F – поиск; «+» – вид доступа разрешен, «-» – вид доступа запрещен.  
2. Таблица разграничения доступа составляется ответственным за ЗИ на основе утвержденного перечня защищаемых ресурсов и **может вестись в электронной форме** для удобства работы ответственного за ЗИ.

**ЖУРНАЛ**  
**учета фактов несанкционированного доступа и воздействия компьютерных вирусов**

№ п/п	Дата и время обнаружения НСД, воздействия компьютерных вирусов, анализа регистрационной информации	Содержание или код события и другие сведения. Результаты анализа регистрационной информации, причина НСД. Последствия факта НСД или воздействия компьютерных вирусов	Решение начальника по факту НСД или воздействия компьютерных вирусов, его подпись, дата время	Принятые меры ответственным за ЗИ
1.	2.	3.	4.	5.
1.	<b>(Пример записи по пункту 29, Методических рекомендаций...)</b> 15:30 10.10.2014 г. обнаружен компьютерный вирус.	Код события операционной системы – 5450. Код события средства ЗИ – 08790. Анализ регистрационной информации показал, что пользователь Sidorov пытался войти под учетной записью администратора.	Провести анализ причин, по которым пользователь пытался войти под учетной записью администратора. подпись, расшифровка подписи и дата	Проведен дополнительный инструктаж с пользователями объекта информатизации кафедры о запрете работы в административном режиме. подпись, расшифровка подписи и дата
2.	<b>(Пример записи по пункту 34, Методических рекомендаций...)</b> 11:30 15.10.2014 г. был вскрыт системный блок зав. № 00000000, учетный № 00000000. Причина: ПЭВМ не включается.	Произведен внешний осмотр ПЭВМ, после вскрытия осмотрена системная плата и блок питания. В результате осмотра установлено, что блок питания неисправен и подлежит замене.	Провести замену блока. подпись, расшифровка подписи и дата	Проведена замена блока питания. После обратной сборки, ПЭВМ опечатаны печатью №№ 0000, 1111. подпись, расшифровка подписи и дата
3.	<b>(Пример записи по пункту 58, Методических рекомендаций...)</b> 09:00 15.10.2014 г.	Обнаружена компрометация пароля на учетную запись Ivanov (кража или утеря).	Провести анализ причин, по которым пароль был скомпрометирован (украден или утерян). подпись, расшифровка подписи и дата.	Проведен анализ причин. Пароль был записан на рабочем столе пользователя. Проведена смена пароля. подпись, расшифровка подписи и дата
4.	<b>(Пример записи по пункту 67, Методических рекомендаций...)</b> 12:00 30.11.2014 г. обнаружен компьютерный вирус.	Код события операционной системы – 5450. Код события САВЗ Dr.Web 9.1 – 587. Анализ регистрационной информации показал, что АРМ был заражен с USB-флэш накопителя I:/	Переместить инфицированный файл в карантин САВЗ Dr.Web 9.1 подпись, расшифровка подписи и дата	Файл отчет.rar перемещен в карантин. подпись, расшифровка подписи и дата
5.	<b>(Пример записи по пункту 74, Методических рекомендаций...)</b> 17:00 05.12.2014 г. проведен ежемесячный анализ журналов операционной системы и LOG-файлов. Нарушений установленного режима обработки информации на объекте информатизации кафедры не выявлено. Подпись ответственного за ЗИ, расшифровка подписи и дата			
6.	Проведено еженедельное обновление БВС САВЗ на объекте информатизации и проверка на наличие компьютерных вирусов. В результате проверки компьютерных вирусов не выявлено. Подпись ответственного за ЗИ, расшифровка подписи и дата			

**Примечание:** В данный журнал наряду с фактами несанкционированного доступа и воздействия компьютерных вирусов вносятся факты информационных воздействий на объекты информатизации АС (ИС, ИТКС), в том числе обнаружения компьютерных атак и внедрения вредоносного программного обеспечения, а также результаты периодического контроля функционирования средств ЗИ.

**Журнал  
учета стирания информации**

№ п/п	Дата и время стирания	Шифр задачи (задания), документа	Оперативная, буферная память	Тип, учетный номер машинного носителя информации	Наименование информационного ресурса (имя файла, набора данных)	Размещение информационного ресурса (том, каталог)	Фамилия и подпись должностного лица, производившего стирание информации	Фамилия и подпись должностного лица, производившего контроль стирания	Примечание
1	10.09.12 17:10	-	-	USB Transend 4Gb Уч. № 000/дсп	Занятия с курсантами 2011 год	I:/	<i>Иванов</i>	Ответственный за ЗИ <i>Жабунов</i>	-
2	15.09.12 11:05	-	АРМ № 1	ЖМД Уч. № 00/дсп	Доклад в ВКС	D:/	<i>Сидоров</i>	Ответственный за ЗИ <i>Жабунов</i>	-

**ЖУРНАЛ**  
**учета машинных носителей информации**

Учетный номер	Тип машинного носителя информации, его заводской номер, номер тома/ количество томов	Принадлежность к средствам автоматизации, номер (шифр) программного средства (задачи)	Гриф секретности	Дата постановки на учет	Учетный номер по журналу предварительного учета или номер входящего документа, дата	Количество экземпляров	Номер экземпляра	Количество рулонов, лент, роликов в экземпляре (штук)	Расписка в получении, дата	Расписка ответственного за учет (работника делопроизводства) в обратном приеме, дата	Отметка об уничтожении или номер исходящего документа, дата
1	2	3	4	5	6	7	8	9	10	11	12
1	ГМД 3.5", зав. № б/н	Материалы по НИР	ДСП	10.06.15	-	1	1	-	Скирда 13.06.15		
2	ЖМД Seagate ST380021A 320 Гб, зав. № 3HV37EXX	Объект информатизации 00 кафедры	НС	13.08.15	-	1	1	-			
3	Компакт-диск CD-R 700 Мб, зав. № 0017	Объект информатизации 00 кафедры	НС	01.09.15	-	1	1	-			
4	Компакт-диск DVD-RW 4.7 Гб, зав. № б/н	Резервная копия, Windows 7	НС	01.09.15	-	1	1	-	Ветрянкин 01.09.15	-	Исх. № 1/155/ВИ (НИ) от 13.09.15
5	USB-flash диск Transcend 32 Гб, зав. № 99000001	Рабочий	НС	01.10.15	-	1	1	-	Варакин 03.09.12		

6	Флэш-карта A-Data SD 8 Гб, зав. № 9930294	Носитель к топогеоде- зическому комплексу	ДСП	02.10.15	-	1	1	-	Глебенко 03.09.12		
7	Ноутбук Asus A52J, зав. № 15G29N0054B1	АРМ № 15	НС	03.12.15	-	1	1	-	Иванов 04.12.15	Жабунов 04.12.15	
8	SSD накопитель 32 Гб Intel SSDMAEMC0402, Зав. № 50015179594C3	АРМ № 34 (ПЭВМ зав. № 1322)	НС	15.12.15	-	1	1	-	Алексеев 15.10.15		

**Примечание:** 1. Каждый экземпляр машинного носителя информации одного учетного номера должен записываться отдельной строкой.

2. Поступившие из других воинских частей МНИ учитываются в журналах учета входящих документов с последующим переносом учета самих МНИ в журнал учета машинных носителей информации с проставлением на них новых реквизитов. Временно поступившие носители учету в журнале учета машинных носителей информации не подлежат.

3. Регистрационный номер наносится на корпус (нерабочую поверхность) МНИ с использованием маркеров или механическим способом. Место маркировки должно обеспечивать возможность его визуального обзора, а способ маркировки — ее сохранность с момента нанесения до окончания срока использования МНИ.

**КНИГА**  
**закрепления и выдачи идентификаторов доступа и паролей**

**I. Идентификаторы доступа**

№ п/п	Вид идентификатора доступа	Заводский (типографический) номер	Номер специального клейма	Условный номер АРМ	Фамилия, инициалы пользователя	Расписка в получении и дата	Расписка в обратном приеме и дата
1	2	3	4	5	6	7	8
3	ЭКН М64	1304	-	АРМ № 23	Шустов Н.Н.	Шустов 01.02.12	
5	ЭКН РИК-2	00001546789	-	АРМ № 129	Семенов К.К.	Семенов 03.02.12	
6	ЭКН USB-токен	687545	-	Ноутбук НДР-25	Семенов К.К.	Семенов 03.08.12	

**II. Пароли на доступ к защищаемым ресурсам<sup>1</sup>**

№ п/п	Наименование средства ВТ, АРМ, защищаемого ресурса	Значение пароля	Срок действия	Расписка в получении (ознакомлении) и дата	Примечание
1	2	3	4	5	6
<p align="center"><u>Семенов К.К.</u> (фамилия и инициалы пользователя)</p>					
1	АПМДЗ АРМ № 129	56g45tn4	01.07.13	Семенов 03.02.12	
2	Ноутбук НДР-25	RTYh56H7	01.03.13	Семенов 03.08.12	
<p align="center"><u>Котов П.П.</u> (фамилия и инициалы пользователя)</p>					
1	ПЭВМ № 6014.28	Hf2ekfd6	01.07.13	Котов 01.02.12	
2	БД ЛВС «Учет», kotov	Kotov8	06.02.12	Котов 06.02.12	

<sup>1</sup> Заполнение раздела II осуществляется на разных листах книги, исключая ознакомление пользователя с паролями других пользователей.

Форма № 12  
(п. 57)

УТВЕРЖДАЮ  
Начальник 00 кафедры  
полковник  
И.Иванов  
«\_\_» апрель 2015 года

ГРАФИК  
смены кодов и паролей на 201 \_\_ год на объекте информатизации 00 кафедры

№ п/п	Месяц											
	Январь	Февраль	Март	Апрель	Май	Июнь	Июль	Август	Сентябрь	Октябрь	Ноябрь	Декабрь
Администраторы												
1.												
Пользователи												
2.												

Ответственный за ЗИ на объекте информатизации 00 кафедры  
капитан

А.Жабунов

Форма № 13  
(п. 33)

УТВЕРЖДАЮ  
Начальник 00 кафедры  
полковник  
И.Иванов  
«\_\_» апрель 2015 года

ГРАФИК  
проведения технического обслуживания на 201 \_\_ год на объекте информатизации 00 кафедры

№ п/п	Месяц											
	Январь	Февраль	Март	Апрель	Май	Июнь	Июль	Август	Сентябрь	Октябрь	Ноябрь	Декабрь
000 лаборатория кафедры												
1.												
помещение № 111 (серверная кафедры)												
2.												

Ответственный за ЗИ на объекте информатизации 00 кафедры  
капитан

А.Жабунев



ОБРАЗЕЦ № 1  
для ПЭВМ, не подключенных к ЛВС

<i>Военно-космическая академия имени А.Ф.Можайского</i>		
(наименование войсковой части или организации)		
<i>АРМ № 55</i>		
(номер АРМ, указание принадлежности к локальной вычислительной сети подразделения или академии)		
<i>3 факультет 33 кафедра 331 учебная лаборатория</i>		
(наименование структурного подразделения)		
<i>ИВАНОВ И.И.</i>	<i>333</i>	
(ответственный пользователь)	(подпись)	(номер личной номерной печати)
<i>СИДОРОВ П.П.</i>	<i>666</i>	
(ответственный за ЗИ на объекте ВТ)	(подпись)	(номер личной номерной печати)
<i>ЖМД № 315/555 нс(дсн) (зав. № LR030975MLK12)</i>		
(учетный и заводской номер МНИ, гриф секретности)		
<i>ЖМД эвакуируется в 1-ю очередь</i>		
(в какую очередь эвакуируется)		

ОБРАЗЕЦ № 2  
для ПЭВМ, объединенных в ЛВС подразделения

<i>Военно-космическая академия имени А.Ф.Можайского</i>		
(наименование войсковой части или организации)		
<i>АРМ № 55 (из состава ЛВС 33 кафедры или ЛВС академии «Электронный ВУЗ»)</i>		
(номер АРМ, указание принадлежности к локальной вычислительной сети подразделения или академии)		
<i>3 факультет 33 кафедра 331 учебная лаборатория</i>		
(наименование структурного подразделения)		
<i>ИВАНОВ И.И.</i>	<i>333</i>	
(ответственный пользователь)	(подпись)	(номер личной номерной печати)
<i>СИДОРОВ П.П.</i>	<i>666</i>	
(ответственный за ЗИ на объекте ВТ)	(подпись)	(номер личной номерной печати)
<i>ЖМД № 315/555 нс(дсн) (зав. № LR030975MLK12)</i>		
(учетный и заводской номер МНИ, гриф секретности)		
<i>ЖМД эвакуируется в 1-ю очередь</i>		
(в какую очередь эвакуируется)		

ОБРАЗЕЦ № 3  
для серверов ЛВС подразделения

<i>Военно-космическая академия имени А.Ф.Можайского</i>		
(наименование войсковой части или организации)		
<i>Файловый сервер № 1 (серверная стойка 33 кафедры)</i>		
(номер АРМ, указание принадлежности к локальной вычислительной сети подразделения или академии)		
<i>3 факультет 33 кафедра 331 учебная лаборатория</i>		
(наименование структурного подразделения)		
<i>ИВАНОВ И.И.</i>	<i>333</i>	
(ответственный пользователь)	(подпись)	(номер личной номерной печати)
<i>СИДОРОВ П.П.</i>	<i>666</i>	
(ответственный за ЗИ на объекте ВТ)	(подпись)	(номер личной номерной печати)
<i>ЖМД № 315/555 нс(дсн) (зав. № LR030975MLK12)</i>		
(учетный и заводской номер МНИ, гриф секретности)		
<i>ЖМД эвакуируется в 1-ю очередь</i>		
(в какую очередь эвакуируется)		

**ОБРАЗЕЦ № 4**  
**для мобильных ПЭВМ (ноутбуков) подразделения**


7 см	<i>Военно-космическая академия имени А.Ф.Можайского</i>		
	<small>(наименование войсковой части или организации)</small>		
	<i>Мобильная ПЭВМ № 1 (из состава ЛВС 33 кафедры или ЛВС академии «Электронный ВУЗ»123)</i>		
	<small>(номер АРМ, указание принадлежности к локальной вычислительной сети подразделения или академии)</small>		
	<i>3 факультет 33 кафедра 331 учебная лаборатория</i>		
	<small>(наименование структурного подразделения)</small>		
	<i>ИВАНОВ И.И.</i>	<i>333</i>	
	<small>(ответственный пользователь)</small>	<small>(подпись)</small>	<small>(номер личной номерной печати)</small>
	<i>СИДОРОВ П.П.</i>	<i>666</i>	
	<small>(ответственный за ЗИ на объекте ВТ)</small>	<small>(подпись)</small>	<small>(номер личной номерной печати)</small>
	<i>ЖМД № 315/555 нс(дсп) (зав. № LR030975MLK12)</i>		
	<small>(учетный и заводской номер МНИ, гриф секретности)</small>		
<i>ЖМД эвакуируется в 1-ю очередь</i>			
<small>(в какую очередь эвакуируется)</small>			

13 см

- Примечание:** 1. На ПЭВМ бирка наносится на верхней поверхности корпуса.  
 2. На мобильную ПЭВМ (ноутбук, нетбук) бирка наносится на верхнюю поверхность корпуса (тыльная сторона монитора)  
 3. Для серверов, которые, как правило, расположены в серверных стойках, бирка оборудуется на внешней боковой стороне стойки на том же уровне, на котором расположен данный сервер.

## Образец маркировки МНИ

3,5 - 4 см



(гриф секретности)

(наименование подразделения)

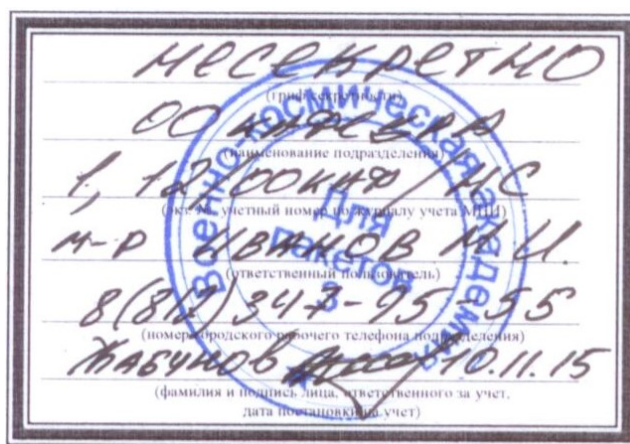
(экз. №, учетный номер по журналу учета МНИ)

(ответственный пользователь)

(номер городского рабочего телефона подразделения)

(фамилия и подпись лица, ответственного за учет,  
дата постановки на учет)

5,5 - 6 см



НЕСЕКРЕТНО

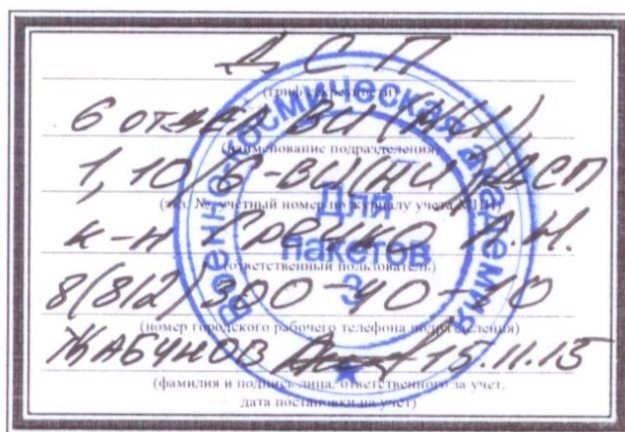
ОО «ИЗВЕЩА

1, 12/00000/НС

М-Р БИВАНОВ М.И.

8(812)347-95-55

ЖАБЧИНОВ 10.11.15



ДСП

6 ОТДЕЛ ВС (МНИ)

1, 10/8-ВЦНЧ/АСП

К-Н ГРЕЧКО В.И.

8(812)300-40-10

ЖАБЧИНОВ 15.11.15

**Примечание:** 1. Способ нанесения штампа № 1 (учетных реквизитов) проводится в зависимости от размеров и типа МНИ:

МНИ типа USB-flash оборудуется биркой или наносится (клеится) на поверхность МНИ;

на МНИ типа CD (DVD)-R(RW) реквизиты наносятся заметным красителем (маркером) на нерабочую поверхность;

на МНИ типа SSD наносится (клеится) бирка.

2. Если МНИ предполагается для обработки информации ограниченного распространения с пометкой «Для служебного пользования», то на нем проставляется уровень конфиденциальности ДСП, для служебной несекретной – НЕСЕКРЕТНО.

УТВЕРЖДАЮ  
Начальник 00 кафедры  
полковник

И.Иванов

«\_\_» апрель 2015 года

### ПЕРЕЧЕНЬ опечатываемых устройств и блоков

---

(наименование объекта информатизации, подразделения)

#### I. Перечень опечатываемых устройств и блоков

№ п/п	Номер помещения	Воинское звание, фамилия и инициалы	Наименование, заводской номер опечатываемого технического средства	Расположение на маршрутной карте	Номера печатей	
					Ответственного за защиту информации	пользователя
1	2	3	4	5	6	7
1	460	Полковник Иванов С.И.	ПЭВМ, зав. № 0111200521	1	41	12
2	459	Подполковник Смирнов В.М.	ПЭВМ, зав. № 170720012	2	41	165
3	459	Подполковник Смирнов В.М.	ПЭВМ, зав. № 2312200201	3	41	165
4	461	г/п Прохорова Л.Н.	ПЭВМ, зав. № 280420001130	4	41	114
5	461	Майор Горячев А.Е.	ПЭВМ, зав. № 170720011	5	41	22
6	461	Майор Сеземов А.В.	ПЭВМ, зав. № 31220011	6	41	21
7	462	Лейтенант Николаев Р.А.	ПЭВМ, зав. № 01/14060488337	7	41	67
8	462	Лейтенант Лоскутова А.В.	ПЭВМ, зав. № 509200207	8	41	28
9	464	Лейтенант Смирнов А.В.	ПЭВМ, зав. № 201044	9	41	45

## II. Маршрутная карта опечатывания устройств и блоков

			9		8 7		1
			464		462		460
				461		459	
				8		8	
				8			
				8		8	

Ответственный за ЗИ на объекте информатизации 00 кафедры  
капитан

А.Жабунув

«\_\_» \_\_\_\_\_ 20\_\_ г.

**Примечание:** Корпуса системных блоков (технологические винты) ПЭВМ опечатаны печатями пользователей и ответственных за защиту информации.

**РАЗРЕШАЮ УНИЧТОЖИТЬ**  
Заместитель начальника Военно-космической  
академии имени А.Ф.Можайского по МТО

полковник

Р.Казаков

« \_\_\_\_ » \_\_\_\_\_ 20\_\_ года

М.П.

от « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

Военно-космическая академия имени А.Ф. Можайского

(условное наименование, а при отсутствии условного наименования записывается полное)

Структурное подразделение \_\_\_\_\_

Материально ответственное лицо \_\_\_\_\_

Форма

Дата

по ОКПО

Код
43
07726295

## АКТ № \_\_\_\_ ОБ УНИЧТОЖЕНИИ ИЗДЕЛИЙ

« \_\_\_\_ » \_\_\_\_\_ 20\_\_ года

г.Санкт-Петербург

Комиссия в составе: **председателя** – \_\_\_\_\_**членов комиссии:** \_\_\_\_\_

\_\_\_\_\_,  
назначенная приказом начальника академии от « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г. № \_\_\_\_ произвела отбор выбракованных в  
процессе эксплуатации нижеперечисленных изделий и установила, что они подлежат уничтожению:

№ п/п	Шифр (индекс) изделия	Заводской (индиви- дуальный) номер	Инвентарный номер	Количе- ство (в штуках, по весу)	Гриф секретности	Инвентарный номер паспорта (формуляра)	Примечание
1	2	3	4	5	6	7	8
1	Seagate 500 Gb	LMJEW968 40G0987	0108859987	2	Несекретно	9076	Акт Ф. ОС-4 № ____ от 06.06.2012 г.
2	USB-flash Transcend 4 Gb.	MNH340G09 87	0100259867	1	Для служебного пользования	-	Акт Ф. ОС-4 № ____ от 06.06.2012 г.

Всего подлежит уничтожению 2 (два) наименования. Записи акта с учетными данными сверены.

Председатель комиссии

(воинское звание)

(подпись)

(расшифровка подписи)

Члены комиссии:

Перечисленные в акте изделия уничтожены путем \_\_\_\_\_ « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.  
(демонтажа, разборки, разрушения, деформирования и т.д.)

Председатель комиссии

(воинское звание)

(подпись)

(расшифровка подписи)

Члены комиссии:

**Заключение:**

В результате проведения осмотра деформированных изделий, указанных в настоящем акте, установлено, что определить их назначение, конструкцию, завод-изготовитель и основные тактико-технические характеристики невозможно.

Председатель комиссии

(воинское звание)

(подпись)

(расшифровка подписи)

Члены комиссии:


Изделия уничтожены после сверки их учетных номеров с записями в акте. В формах учета отметки об уничтожении изделий произвел ответственный за учет изделий (МНИ)

(подпись, инициалы и фамилия лица ответственного за учет изделий (МНИ))

« \_\_\_\_ » \_\_\_\_\_ 20\_\_ года

**Пояснение к форме**

1. Акт об уничтожении изделий применяется для оформления результатов проведения работ по уничтожению изделий путем разборки, деформации или другим иным способом.

2. Уничтожение изделий производится после утверждения актов о списании материальных ценностей.

3. Уничтожение изделий производится комиссионно.

Состав комиссии:

Председатель комиссии – начальник структурного подразделения академии;

Члены комиссии:

– ответственный за ЗИ в подразделении академии;

– материально ответственное лицо;

– представитель отделения МТО.

4. Оформленный акт подписывается членами комиссии и предоставляется на утверждение заместителю начальника академии. Подпись, утвердившего акт заверяется гербовой печатью академии.

5. Акт оформляется в двух экземплярах:

– первый экземпляр акта передается в отдел учета материальных средств ФС;

– второй – материально ответственному лицу.

**Примечание.** 1. В графе «Примечание» акта об уничтожении изделий записываются номера и даты актов о списании объектов основных средств (Ф.№ ОС-4), по которым списаны изделия (при наличии такого акта).

2. После уничтожения изделия (жесткого диска и (или) флэшки) в журнале учета МНИ в графе 12 указываются учетные номера актов об уничтожении ([форма № 10](#)).

**ПРИКАЗ  
НАЧАЛЬНИКА ВОЕННО-КОСМИЧЕСКОЙ АКАДЕМИИ  
ИМЕНИ А.Ф.МОЖАЙСКОГО**

№ \_\_\_\_\_

\_\_\_\_\_ 201\_\_ года

г. Санкт-Петербург

**О вводе в эксплуатацию объекта информатизации 00 кафедры Военно-космической академии  
имени А.Ф.Можайского**

В соответствии с Руководством по защите информации от несанкционированного доступа в Вооруженных Силах Российской Федерации, утвержденного приказом Министра обороны Российской Федерации 2013 года № 011 (РЗИ – 2013), на основании положительных выводов акта готовности системы ЗИ на объекте информатизации 00 кафедры (уч. № 00 от 00.00.2000 г.) **П Р И К А З Ы В А Ю :**

1. Ввести в эксплуатацию объект информатизации 00 кафедры в составе, указанном в приложении № 1 к настоящему приказу с 00.00.2000 года.

2. Утвердить список должностных лиц объекта информатизации 00 кафедры (приложение № 2 к настоящему приказу).

3. Утвердить список должностных лиц (пользователей) объекта информатизации 00 кафедры (приложение № 3 к настоящему приказу).

4. Время работы пользователей на объекте информатизации 00 кафедры установить:

в рабочие дни – с 8:30 до 20:00;

по субботам – с 9:00 до 15:00.

5. Разрешить на объекте информатизации обработку:

на АРМ №№ 16-18 – информации ограниченного распространения с пометкой «Для служебного пользования»;

на АРМ №№ 1-15 – служебной несекретной информации.

6. Выполнение мероприятий по ЗИ от НСД на объекте информатизации 00 кафедры осуществлять в соответствии с инструкцией по ЗИ и Методическими рекомендациями по защите служебной информации от НСД в Военно-космической академии имени А.Ф.Можайского, утвержденными приказом начальника академии от 00.00.2000 года № 000, а также:

на АРМ №№ 16-18, обрабатывающих информацию ограниченного распространения с пометкой «Для служебного пользования», в соответствии с классом защищенности 1Г;

на АРМ №№ 1-15, обрабатывающих служебную несекретную информацию, в соответствии с классом защищенности 1Д.

7. Исключить несанкционированный вынос СВТ и МНИ объекта информатизации 00 кафедры за пределы контролируемой зоны академии и выход с СВТ в ИТКС ОП «Интернет».

8. В целях выполнения мероприятий по ЗИ от НСД проводить проверку функционирования всех средств ЗИ объекта информатизации не реже одного раза в год внутрипроверочной комиссией академии с составлением акта.

9. Считать утратившим силу приказ начальника академии 2014 года № 111 (крайний приказ о вводе объекта ВТ подразделения в эксплуатацию).

10. Контроль исполнения приказа возложить на заместителя начальника академии<sup>2</sup> через службу ЗГТ академии.

11. Приказ довести до должностных лиц академии в части касающейся.

**НАЧАЛЬНИК ВОЕННО-КОСМИЧЕСКОЙ АКАДЕМИИ  
ИМЕНИ А.Ф.МОЖАЙСКОГО  
генерал-майор**

**М.Пеньков**

<sup>2</sup> Если объект информатизации принадлежит ОРЛС, СО, СЗГТ, МС, ЮС, ФЭС, ОК, УС или базе (ОУП), то исполнение возлагается на заместителя начальника академии;

если объект информатизации принадлежит УМО, О (ОНР), ОфК, 1-9 факультету, ФППК, СПО, СФ, 101-117 ОАК, кафедре РЯ, ВИ (НИ), ОТСО или РИО – на заместителя начальника академии по учебной и научной работе.



**СОСТАВ**  
объекта информатизации 00 кафедры Военно-космической академии  
имени А.Ф.Можайского

№ п/п	Наименование и состав оборудования	Заводской (серийный) номер
<b>3 этаж учебного корпуса № 1, 00 кафедра, помещение № 000</b>		
АРМ № 1 (начальника подразделения)		
14.	Системный блок Aquarius Pro P30 S61	2140313629126-0024
15.	Клавиатура Logitech MK 120-USB	90223811958178
16.	Манипулятор «мышь» оптическая Logitech M-U0026	7K2914
17.	Монитор AOC E960Srda	FMJE1HA046039
18.	Источник бесперебойного питания APC BK500-RS	4B1326P49851
19.	Сетевой фильтр Defender ESS	б/н
20.	Принтер Xerox Phaser 3160N	3960454196
АРМ № 2 (зам. начальника подразделения)		
21.	Системный блок Asus	36457586789689
22.	Клавиатура Logitech MK 120-USB	dfgbsrgyyet44t
23.	Манипулятор «мышь» оптическая Logitech M-U0026	4353453434
24.	Монитор AOC E960Srda	rthfhfghs43452
25.	Источник бесперебойного питания APC BK500-RS	t43w53534tet4
26.	Сетевой фильтр Defender ESS	б/н
27.	Принтер Xerox Phaser 3160N	453t4gd4t236
АРМ № 3 (преподавателя, лаборанта и т.д.)		
28.	Системный блок Samsung	24352trswrz5
29.	Клавиатура Logitech MK 120-USB	54362447657538
30.	Манипулятор «мышь» оптическая Logitech M-U0026	537457247624
31.	Монитор AOC E960Srda	2624585362
32.	Источник бесперебойного питания APC BK500-RS	4645675786535
33.	Сетевой фильтр Defender ESS	б/н
34.	Принтер Samsung	356753798769

Начальник подразделения (объекта информатизации)  
полковник

И.Иванов

СПИСОК  
должностных лиц объекта информатизации 00 кафедры

№ п/п	Занимаемая воинская должность	Воинское звание, фамилия и инициалы	Специальные обязанности, возлагаемые на должностного лица
1.	Начальник 00 кафедры	полковник ИВАНОВ И.И.	Начальник объекта информатизации
2.	Преподаватель 00 кафедры	капитан ЖАБУНОВ А.А.	Ответственный за защиту информации
3.	Начальник 009 лаборатории	лейтенант ЗАЗУЛЯ О.О.	Ответственный за эксплуатацию технических и программных средств

Начальник подразделения (объекта информатизации)  
полковник

И.Иванов

СПИСОК  
должностных лиц (пользователей) объекта информатизации 00 кафедры

№ п/п	Занимая должность	Воинское звание, фамилия, имя и отчество пользователя	Логическое имя
1.	Преподаватель 00 кафедры	подполковник ВЫХУХОЛИДЗЕ Бахруз Гиляшотович	Vihuholidje B.G.
2.	Старший научный сотрудник 000 лаборатории	капитан ПЕРЕПЕЛИЦА Андрей Геннадьевич	Perepelica A.G.
3.	Лаборант 000 кафедры	СИДОРОВА Любовь Евгеньевна	Sidorova 153

Начальник подразделения (объекта информатизации)  
полковник

И.Иванов

УТВЕРЖДАЮ

Заместитель начальника академии  
полковник

С.Чистяков

« \_\_\_\_ » марта 2015 года

## АКТ

**вскрытия системного блока из состава объекта информатизации 00 кафедры  
Военно-космической академии имени А.Ф.Можайского**

« \_\_\_\_ » февраля 2015 года

г. Санкт-Петербург

В соответствии с требованиями «Руководства по защите информации от несанкционированного доступа в Вооруженных Силах Российской Федерации», утвержденного приказом Министра обороны Российской Федерации 2013 года № 011 (РЗИ – 2013) 00 февраля 2015 года специалисты в составе: председателя комиссии начальника 000 кафедры полковника ИВАНОВА И.И., членов комиссии: офицера по обеспечению безопасности информации и режима секретности службы защиты государственной тайны (ЗГТ) академии старшего лейтенанта БЕЛЯКОВА М.И., ответственного за защиту информации (ЗИ) капитана ЖАБУНОВА А.А., материально ответственного лица лейтенанта СИДОРЕНКО В.В. и инженера ЗАО «РАМЭК-ВС» СЕНЧЕНКО И.М.,<sup>3</sup> провели вскрытие системного блока Aquarius Pro P30 S61 (зав. № 12345678-1234) для проведения ремонтных работ (технического обслуживания). Личные номерные печати, которыми опечатан системный блок (корпус) технического средства перед вскрытием – 111, 2222, номер заводской печати – 001127173<sup>4</sup>.

В ходе визуальной проверки системного блока внешних повреждений не выявлено (либо выявлены определенные неисправности с их кратким описанием).

При нажатии на кнопку включения компьютера загрузка АПМЗД «ЦЕНТУРИОН» и, соответственно BIOS, не происходит. Предполагаемая причина – неисправность блока питания или системной платы.<sup>5</sup>

**Вывод:** системный блок, указанный в акте подлежит передаче инженеру ЗАО «РАМЭК-ВС» для проведения ремонтных работ. Жесткий диск WD5000AAKX – 08330055 (зав. № C2E0000000) подлежит передаче на объект информатизации на хранение ответственному за ЗИ капитану Жабунову А.А.

Председатель комиссии:

полковник

И.Иванов

Члены комиссии:

капитан

А.Жабунов

старший лейтенант

М.Беляков

лейтенант

В.Сидоренко

И.Сенченко

<sup>3</sup> В случае, если техническое средство(а) состоит(ят) на гарантии в сторонней организации и для его ремонта на месте прибыл представитель сторонней организации (либо прибыл для доставки технического средства в стороннюю организацию для проведения ремонтных работ), в состав комиссии включается должностное лицо (представитель) этой сторонней организации, оказывающей услуги по ремонту.

<sup>4</sup> Печать завода-изготовителя указывается при ее наличии.

<sup>5</sup> В данном абзаце описываются конкретные неисправности, либо их признаки и предполагаемая причина.

*В приложении к сопроводительному письму указывается:*

Приложение: CD-R № 000/000нс(дсп), экз. № 1 несекретно *(или)* (ДСП), только адресату.

На CD-R № 000/000нс(дсп) записано:

файл «Отчет1.rar», контрольная сумма (md5) e6d7b90fbe0e0b23c0ee1a17561f1ba4;

файл «Отчет2.rar», контрольная сумма (md5) d5d2622d163db0eb3c5ba706e5c3ac.

Указанный МНИ проверен на наличие вредоносного ПО САВЗ Dr.Web Security Space<sup>6</sup>, вредоносное ПО не обнаружено.

Начальник \_\_\_\_\_

«\_\_» \_\_\_\_\_ 20\_\_ года

Исх. № \_\_\_\_\_

---

<sup>6</sup> Указывается то средство антивирусной защиты, которым проверялись пересылаемые файлы (наборы данных).

Заместителю начальника академии

## Рапорт

Представляю доклад о проведенных мероприятиях по защите информации на объекте информатизации 00 кафедры по состоянию на 10 июля 2015 года:

1. На всех СВТ подразделения в течении месяца были установлены еженедельные обновления баз вирусных сигнатур САВЗ (01.07.15<sup>7</sup>, 08.07.15, 15.07.15, 22.07.15, 29.07.15). После установки обновлений проведены проверки СВТ на наличие компьютерных вирусов. В результате проверок фактов воздействия компьютерных вирусов и программных средств скрытого информационного воздействия не установлено.<sup>8</sup>

2. Проведены проверки на наличие НСД к защищаемым ресурсам. Фактов НСД не установлено.<sup>9</sup>

Начальник 00 кафедры  
полковник

И.Иванов

« \_\_\_\_ » \_\_\_\_\_ 20 \_\_ г.

**Примечание.** 1. Рапорт представляется к 30 числу каждого месяца в службу ЗГТ академии.

---

<sup>7</sup> В скобках указаны даты установки обновлений на СВТ.

<sup>8</sup> В случае, если за отчетный период были выявлены воздействия, то следует указать: дату и время обнаружения, Ф.И.О. обнаружившего лица, кому доложено и принятые меры пользователем и ответственным за ЗИ. Сделать соответствующие записи в журнале учета фактов НСД и воздействия компьютерных вирусов (форма № 8).

<sup>9</sup> В случае, если за отчетный период были выявлены факты НСД к защищаемым ресурсам, в том числе изменение конфигурации и(или) несанкционированное вскрытие технических средств (нарушение целостности печатей, пломб, наклеек, защитных знаков), то следует указать: дату и время обнаружения, Ф.И.О. обнаружившего лица, кому доложено и принятые меры пользователем и ответственным за ЗИ. Сделать соответствующие записи в журнале учета фактов НСД и воздействия компьютерных вирусов ([форма № 8](#)).

Проверка на наличие НСД к защищаемым ресурсам проводится путем анализа журналов операционных систем и журналов средств ЗИ.

**ТИПОВАЯ СТРУКТУРА И ТРЕБОВАНИЯ  
к содержанию инструкции по защите информации  
в на объекте информатизации подразделения академии**

**СОГЛАСОВАНО**

Офицер по ОБИ и РС службы защиты  
государственной тайны академии  
старший лейтенант

М.Беляков

« \_\_\_\_ » марта 2015 года

**УТВЕРЖДАЮ**

Начальник 00 факультета  
полковник

С.Сидоров

« \_\_\_\_ » марта 2015 года

**ИНСТРУКЦИЯ**

**по защите информации** \_\_\_\_\_

(наименование объекта информатизации, подразделения)

Инструкция по защите информации разрабатывается применительно к условиям эксплуатации объекта информатизации подразделения и должна отражать конкретные мероприятия по защите информации, порядок проведения и контроля за их выполнением, действия и ответственность должностных лиц подразделения академии.

Примерный перечень разделов, которые отражаются в инструкции по защите информации, и их содержание:

**I. ОБЩИЕ ПОЛОЖЕНИЯ**

Раздел содержит сведения о правовых актах Министерства обороны и других документах, на основании которых разработана данная инструкция, и общие сведения об объектах информатизации (СВТ) подразделения (их принадлежность к АС, предназначение, максимальная степень секретности информации, обрабатываемой на объекте информатизации).

**II. ОБЯЗАННОСТИ ДОЛЖНОСТНЫХ ЛИЦ ПО ЗАЩИТЕ ИНФОРМАЦИИ  
ОТ НСД НА ОБЪЕКТЕ ИНФОРМАТИЗАЦИИ**

В разделе отражаются обязанности начальника объекта информатизации, ответственного за ЗИ, ответственных за эксплуатацию технических и программных СВТ и пользователей. Определяется, что запрещается пользователям при эксплуатации технических и программных СВТ объекта информатизации.

**III. ОРГАНИЗАЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НСД НА ОБЪЕКТЕ ВТ**

Раздел содержит:

порядок ввода в эксплуатацию объекта информатизации и допуска пользователей к самостоятельной работе;

перечень средств ЗИ и выполняемые ими функции; порядок применения средств ЗИ;

порядок разграничения доступа к защищаемым ресурсам объекта информатизации, параметры паролирования (в том числе длина, типы символов и периодичность смены паролей (кодов) в средствах ЗИ);

порядок копирования (размножения) и стирания информации;

порядок допуска пользователей к ресурсам объекта информатизации подразделения (СВТ, информационным и вычислительным ресурсам);

порядок сдачи под охрану помещений с расположенными в них техническими средствами объекта информатизации (если помещение оборудовано техническими средствами охраны и предусмотрена его сдача под охрану);

порядок действий должностных лиц при компрометации паролей (кодов), утере идентификаторов доступа и паролей;

порядок проведения технического обслуживания и ремонта программных и технических средств, уборочных работ в помещениях с расположенными в них техническими средствами объекта информатизации; порядок опечатывания устройств и блоков СВТ; порядок действий должностных лиц в случае поступления сигнала о НСД к защищаемым ресурсам.

#### **IV. ОРГАНИЗАЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ВОЗДЕЙСТВИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ**

Раздел содержит:

порядок осуществления антивирусной защиты;

порядок получения и применения БВС САВЗ;

периодичность проведения проверок СВТ на отсутствие компьютерных вирусов (съёмные МНИ подлежат быстрой проверке при подключении к СВТ, а МНИ, встроенные в технические средства (ПЭВМ) – не реже одного раза в неделю);

порядок действий должностных лиц при обнаружении компьютерных вирусов на СВТ.

#### **V. ПОРЯДОК УЧЕТА, ХРАНЕНИЯ МНИ И МАШИННЫХ (ВЫХОДНЫХ) ДОКУМЕНТОВ И ОБРАЩЕНИЯ С НИМИ**

В разделе отражаются:

порядок учета, хранения, выдачи, маркировки и уничтожения МНИ;

порядок формирования бумажных документов, содержащих информацию ограниченного распространения с пометкой «Для служебного пользования» (в случае, если на объекте информатизации или отдельных СВТ разрешена обработка документов «Для служебного пользования»);

порядок хранения эталонных МНИ (лицензионных дисков с программным обеспечением или информационно-справочными ресурсами).

#### **VI. КОНТРОЛЬ ЗА ОРГАНИЗАЦИЕЙ И СОСТОЯНИЕМ РАБОТЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОТ НСД НА ОБЪЕКТЕ ИНФОРМАТИЗАЦИИ**

В разделе отражается, кто и когда имеет право проверки вопросов ЗИ на объекте информатизации (служба ЗГТ академии, ответственный за ЗИ и начальник объекта информатизации), как она проводится, каким документом оформляются результаты (отражаются в ежемесячном рапорте о состоянии ЗИ в подразделении).

Определяется порядок и сроки проведения проверки системных журналов операционных систем, журналов средств ЗИ и log-файлов на каждом СВТ (но не реже 1 раза в месяц).

#### **VII. ДЕЙСТВИЯ ЛИЧНОГО СОСТАВА НА СЛУЧАЙ СТИХИЙНОГО БЕДСТВИЯ**

Раздел разрабатывается в соответствии с требованиями, установленными в пункте 52 настоящего Руководства (если не разработана отдельная инструкция).

Начальник 00 кафедры (начальник объекта информатизации)  
полковник

И.Иванов

«\_\_\_» \_\_\_\_\_ 20\_\_ г.



УТВЕРЖДАЮ  
Заместитель начальника академии  
полковник  
С.Чистяков

« \_\_\_\_ » марта 2015 года

**АКТ**  
**вывода из эксплуатации объекта информатизации 000 кафедры (или отдельных СВТ)**  
**Военно-космической академии имени А.Ф.Можайского**

« \_\_\_\_ » марта 2015 года

г. Санкт-Петербург

Комиссия в составе: председателя комиссии начальника 000 кафедры полковника ИВАНОВА И.И., членов комиссии: начальника узла связи академии майора ДУБОВА В.В., офицера по обеспечению безопасности информации и режима секретности службы защиты государственной тайны (ЗГТ) академии старшего лейтенанта БЕЛЯКОВА М.И., ответственного за защиту информации (ЗИ) капитана ЖАБУНОВА А.А. и ответственного за эксплуатацию программных и технических средств на объекте информатизации лейтенанта ЗАЗУЛЯ О.О., провела мероприятия по выводу из эксплуатации объекта информатизации 000 кафедры (или отдельных СВТ) в составе:

1. Состав технических средств объекта информатизации, выводимых из эксплуатации:

№ п/п	Наименование и состав основного оборудования	Заводской (серийный) номер
1.	2.	3.
<b>3 этаж учебного корпуса № 1, помещение № 514</b>		
<b>АРМ № 1</b>		
1.	Системный блок Aquarius Pro P30 S61	MLGK875JNBKJ
2.	Клавиатура Logitech MK 120-USB	3KM2HN4M5K
3.	Манипулятор «мышь» оптическая Logitech M-U0026	24MM2K56M43
4.	Монитор AOC E960Srda	MLLKIOOLFKI67
5.	Источник бесперебойного питания APC BK500-RS	4B1326P49851
6.	Сетевой фильтр Defender ESS	б/н

2. В ходе работы комиссии проводились следующие работы:

выгрузка (копирование) защищаемых ресурсов на внешние МНИ (уч. №№ 0/000, 1/111);  
стирание (или низкоуровневое форматирование в случае полного стирания жестких дисков) информации с МНИ (уч. №№ 0000, 1111), указанных в составе технических средств объекта информатизации;  
ведение учетной документации по ЗИ закрыто, документы, содержащие информацию ограниченного распространения с пометкой «Для служебного пользования» отобраны на уничтожение.

**Вывод:** мероприятия по ЗИ проведены в полном объеме и позволяют вывести из эксплуатации технические средства объекта информатизации 000 кафедры.

Председатель комиссии:

полковник

И.Иванов

Члены комиссии:

майор

В.Дубов

капитан

А.Жабун

старший лейтенант

М.Беляков

лейтенант

О.Зазуля

## СПИСОК

должностных лиц, имеющих право утверждения документов по защите информации на объектах информатизации соответствующих подразделений

Таблица 3

№ п/п	Наименование подразделений	Должностное лицо, утверждающее документы
1.	Стреловой отдел	Заместитель начальника академии
2.	Служба защиты государственной тайны	
3.	Медицинская служба	
4.	Юридическая служба	
5.	Финансово-экономическая служба	
6.	Отдел кадров	
7.	Узел связи	
8.	Учебно-методический отдел	Заместитель начальника академии по учебной и научной работе
9.	Отдел (организации научной работы и подготовки научно-педагогических кадров)	
10.	Офицерские курсы (по подготовке специалистов с высшей оперативно-тактической подготовкой)	
11.	Факультет переподготовки и повышения квалификации	
12.	Факультет среднего профессионального образования	
13.	Специальный факультет	
14.	Общеакадемические кафедры	
15.	Кафедра русского языка	
16.	Отдел технических средств обучения	
17.	Редакционно-издательский отдел	
18.	Отдел материально-технического обеспечения	Заместитель начальника академии по материально-техническому обеспечению
19.	Отдел по работе с личным составом	Заместитель начальника академии по работе с личным составом
20.	1-9 факультеты	Начальники факультетов
21.	Военный институт (научно-исследовательский)	Начальники управлений
22.	База (ОУП) (п. Лехтуси)	Начальник Базы (ОУП)
23.	Учебный центр (ЗРВ, п. Войсковицы)	Начальник учебного центра
24.	Центр подготовки специалистов (рРТВ, г. Владимир)	Начальник центра

**ОСНОВНЫЕ ТРЕБОВАНИЯ**  
**к парольной защите на объектах информатизации академии**

Таблица 4

Уровень конфиденциальности обрабатываемой информации	Минимальная длина пароля (буквенно- цифровых символов)	Допустимое число неудачных попыток неправильного ввода пароля	Максимальная периодичность смены паролей
Для служебного пользования	8	Не более 5	1 раз в 6 месяцев
Служебная несекретная информация	6	Не более 8	1 раз в год

**НАЧАЛЬНИК СЛУЖБЫ – ПОМОЩНИК НАЧАЛЬНИКА АКАДЕМИИ**  
**ПО ЗАЩИТЕ ГОСУДАРСТВЕННОЙ ТАЙНЫ**  
**ПОЛКОВНИК**

**О.Варсегов**