«УТВЕРЖДАЮ»
ПЕРВЫЙ ПРОРЕКТОР

_____ С.Н. АЛТУНИН
«30» апреля 2019 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДИПЛОМАТИЧЕСКОЙ АКАДЕМИИ МИД РОССИИ

ИНФОРМАЦИЯ О ДОКУМЕНТЕ

Номер документа			
Версия			
Утвержден			
Статус	☐ действующий	☐ временный	☐ отменен
Распространение	☐ ограничено	☐ конфиденциально	☐для персонала
	☐ версия для печати		
Ответственный разработчик		**Телефон**	

ОГЛАВЛЕНИЕ

ТЕРМИНЫ И СОКРАЩЕНИЯ

Использованные в настоящем документе термины и сокращения трактуются следующим образом:

Академия	Дипломатическая академия МИД России
Управление ИТ	Управление информационной технологий
ПО	Программное обеспечение
ИБ	Информационная безопасность
Рабочая станция	Стационарный компьютер корпоративной сети
ОС	Операционная система

Расшифровка понятий информационных ресурсов:

Сервер - аппаратно-программный комплекс, исполняющий функции хранения и обработки запросов пользователей и не предназначенный для локального доступа пользователей (выделенный сервер, маршрутизатор и другие специализированные устройства) ввиду высоких требований по обеспечению надежности, степени готовности и мер безопасности информационной системы Академии.

Рабочая станция – персональный компьютер (терминал), предназначенный для доступа пользователей к ресурсам Автоматизированной системы Академии, приема передачи и обработки информации.

Автоматизированная система (АС) - совокупность программных и аппаратных средств, предназначенных для хранения, передачи и обработки данных и информации, и производства вычислений.

Системный администратор - должностное лицо, в обязанности которого входит обслуживание всего аппаратно-программного комплекса Академии, управление доступом к сетевым ресурсам, а также поддержание требуемого уровня отказоустойчивости и безопасности данных, их резервное копирование и восстановление.

Пользователь - сотрудник Академии, использующий ресурсы информационной системы для выполнения должностных обязанностей.

Учетная запись - информация о сетевом пользователе: имя пользователя, его пароль, права доступа к ресурсам и привилегии при работе в системе. Учетная запись может содержать дополнительную информацию (Адрес электронной почты, телефон и т.п.).

Пароль - секретная строка символов (букв, цифр, специальных символов), предъявляемая пользователем компьютерной системе для получения доступа к данным и программам. Пароль является средством защиты данных от несанкционированного доступа.

Изменение полномочий - процесс создания, удаления, внесения изменений в учетные записи пользователей АС, создание, удаление изменение наименований почтовых ящиков и адресов электронной почты, создание, удаление изменение групп безопасности и групп почтовой рассылки, а также другие изменения, приводящие к расширению (сокращению) объема информации либо ресурсов доступных пользователю АС.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Информация о документе Академии разработана в целях определения требований по безопасности в области информационных технологий.

1.2. Информационная безопасность является одним из составных элементов комплексной безопасности Академии. Под информационной безопасностью Академии понимается состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности.

1.3. Информационная безопасность - деятельность, направленная на обеспечение защищенного состояния объекта информации, в том числе объектов автоматизированных и телекоммуникационных систем, противодействия техническим разведкам, включающая комплексные, криптографические, компьютерные, организационные, технические средства защиты.

1.4. Обеспечение информационной безопасности осуществляется по следующим направлениям:

-правовая защита - процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;

-организационная защита -это регламентация деятельности и взаимоотношений исполнителей на нормативно - правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба;

-инженерно-техническая защита - это использование различных технических средств, препятствующих нанесению ущерба.

1.5. Информационная безопасность включает:

-защиту интеллектуальной собственности Академии;

-защиту компьютеров, локальных сетей и сети подключения к системе Интернета;

-организацию защиты конфиденциальной информации, в т. ч. персональных данных работников и обучающихся;

-учет всех носителей конфиденциальной информации.

Информационная безопасность Академии должна обеспечивать:

-конфиденциальность (защиту информации от несанкционированного раскрытия или перехвата);

-целостность (точность и полноту информации и компьютерных программ);

-доступность (возможность получения пользователями информации в пределах их компетенции).

К объектам информационной безопасности Академии относятся:

- информационные ресурсы, содержащие документированную информацию, в соответствии с перечнем сведений конфиденциального характера;

- информацию, защита которой предусмотрена законодательными актами РФ, в т. ч. и персональные данные;

- средства и системы информатизации, программные средства, автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку-хранение и передачу информации с ограниченным доступом.

Правовую основу Положения составляют:

-Конституция Российской Федерации;

-Федеральный закон «О безопасности» от 28.12.2010 № 390-ФЗ;

-Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ;

-Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ;

-Федеральный закон «Об информации, информационных технологиях о защите информации» от 26.07.2006 № 149-ФЗ;

-Федеральный закон «О персональных данных» от 27.07.06 № 152-ФЗ (в ред. от 27.07.2011)-ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью" (утв. Приказом Ростехрегулирования от 29.12.2005 N 447-ст)-другие законодательные акты, руководящие и нормативно-методические документы Российской Федерации в области обеспечения информационной безопасности.

1.6. Информация о документе Академии определяет принципы, подходы и требования, направленные на обеспечение информационной безопасности в следующих областях:

- Использования рабочих станций;
- Использования ноутбуков;
- Эксплуатации серверов;
- Эксплуатации активного сетевого оборудования;
- Проведения аудита безопасности;
- Классификации данных;
- Применения парольной защиты;
- Резервного копирования и восстановления данных;
- Организации удаленного доступа;
- Предоставления доступа сторонних организаций к ресурсам Академии;
- Соблюдения лицензирования ПО;
- Предоставления / удаления / изменения прав доступа к системам;
- Контроля физического доступа к ИТ- инфраструктуре;
- Реагирования на инциденты в области ИБ.

1.7. Настоящий документ является обязательным для всех подразделений Академии.

1.7.1. К сотруднику Академии, нарушившему требования настоящей политики, могут быть применены дисциплинарные меры, предусмотренные действующим трудовым законодательством, вплоть до увольнения, а так же привлечение к административной ответственности в результате нанесения материального или морального ущерба Академии.

1.7.2. Определение дисциплинарных мер осуществляется руководством Академии в соответствии с последствиями и масштабом нанесенного ущерба, которые повлекло нарушение политики.

1.8. Ответственность за контроль исполнения положений настоящего документа несет начальник Управления информационных технологий Академии и отчитывается перед Первым проректором в случаях нарушения исполнения данного документа.

2. ПОЛИТИКА БЕЗОПАСНОСТИ РАБОЧИХ СТАНЦИЙ

2.1. Цель

2.1.1. Настоящая политика определяет требования к безопасности рабочих станций пользователей Академии.

2.1.2. Выполнение этой политики минимизирует вероятность несанкционированного доступа к конфиденциальной информации Академии, обрабатываемой на рабочих станциях.

2.2. Область действия

2.2.1. Политика обязательна для всех сотрудников Академии, имеющих доступ к рабочим станциям.

2.3. Требования политики

2.3.1. Каждая рабочая станция должна иметь уникальное сетевое имя. Правила именования рабочих станций должны быть едиными, универсальными и простыми.

2.3.2. В Академии должен поддерживаться актуальный реестр используемых рабочих станций, в котором должна быть информация об ответственном пользователе и конфигурации.

2.3.3. Рабочие станции и периферийное оборудование предоставляются пользователям исключительно для выполнения должностных обязанностей. Сотрудники несут ответственность за использование рабочих станций и других ресурсов Академии в личных целях.

2.3.4. Требования к безопасности при использовании рабочих станций сотрудниками Академии должны определяться отдельными внутренними Положениями. Существующий в Академии способ ознакомления должен обеспечивать доведение указанных Положений до каждого пользователя.

2.3.5. Пользователи обязаны сообщать обо всех фактах, связанных с возможным нарушением информационной безопасности их рабочих станций в Управление информационных технологий.

2.3.6. В случае утраты или порчи рабочей станции в Академии должно проводится служебное расследование силами сотрудников Управления информационных технологий.

3. ПОЛИТИКА БЕЗОПАСНОСТИ НОУТБУКОВ

3.1. Цель

3.1.1. Настоящая политика определяет требования к безопасности ноутбуков мобильных пользователей Академии.

3.1.2. Выполнение этой политики минимизирует вероятность несанкционированного доступа к конфиденциальной информации Академии, обрабатываемой на переносных компьютерах.

3.2. Область действия

3.2.1. Политика обязательна для всех сотрудников Академии, использующих ноутбуки.

3.3. Требования политики

3.3.1. Каждый ноутбук должен иметь уникальное сетевое имя. Правила именования ноутбуков должны быть аналогичны правилам наименования стационарных рабочих станций.

3.3.2. В Академии должен поддерживаться актуальный реестр используемых ноутбуков, в котором должна содержаться информация об ответственном пользователе и конфигурации ноутбука.

3.3.3. Ноутбуки предоставляются пользователям исключительно для выполнения должностных обязанностей. Сотрудники несут ответственность за использование ноутбуков в личных целях.

3.3.4. Требования к безопасности при использовании ноутбуков сотрудниками Академии должны определяться отдельными внутренними Положениями. Существующий в Академии способ ознакомления должен обеспечивать доведение указанных Положений до каждого пользователя.

3.3.5. Пользователи обязаны сообщать обо всех фактах, связанных с возможным нарушением информационной безопасности их ноутбуков в управление информационных технологий.

3.3.6. В случае утраты или порчи ноутбука в Академии должно проводится служебное расследование силами сотрудников Управления информационных технологий.

4. ПОЛИТИКА БЕЗОПАСНОСТИ СЕРВЕРОВ

4.1. Цель

4.1.1. Настоящая политика определяет конфигурацию и требования к поддержке серверов, находящихся в собственности Академии и используемых в ее сети.

4.1.2. Выполнение этой политики минимизирует вероятность нарушения режима информационной безопасности в отношении серверов Академии.

4.2. Область действия

4.2.1. Политика охватывает все серверное оборудование, принадлежащие Академии и размещенное на любой из ее технологических площадок. Политика обязательна для выполнения в Академии.

4.3. Требования политики

4.3.1. Каждый сервер, установленный в сети Академии, должен быть закреплен за сотрудником Управления информационных технологий, ответственным за администрирование / поддержку сервера.

4.3.2. В обязанности сотрудника, ответственного за администрирование / поддержку входит поддержание конфигурации сервера в соответствии с внутренними стандартами. Стандарты аппаратной и программной конфигурации серверов определяются текущими бизнес-задачами и утверждаются руководством Академии и Начальника управления.

4.3.3. В Обществе должен поддерживаться реестр серверного оборудования. По каждому серверу должна быть зарегистрирована следующая минимальная информация:

- сетевое имя сервера;
- адрес (адреса) во внутренней сети;
- физическое местоположение сервера;
- производитель оборудования и версия ОС;
- ответственный за администрирование сервера;
- ответственный за резервное копирование информации;

- основные функции и информационные системы.

4.3.4. Информация об изменениях в конфигурации серверов должна своевременно обновляться сотрудниками, ответственными за серверное оборудование. Логические и физические связи серверов должны быть отражены в общей схеме сети.

4.3.5. Каждый сервер должен быть промаркирован (например, наклейками на передней панели), так, чтобы его можно было однозначно идентифицировать. Принцип маркирования должен быть унифицирован и донесен до сведения всех сотрудников, работающих с серверами.

4.3.6. В конфигурации сервера неиспользуемые службы / сервисы / приложения должны быть отключены / удалены.

4.3.7. Доступ к сервисам должен журналироваться и защищаться с использованием методов контроля доступа.

4.3.8. Обновления средств безопасности должны устанавливаться сразу после их появления, если это не влияет на выполнение критических приложений.

4.3.9. Встроенная учетная запись администратора должна быть переименована там, где это возможно.

4.3.10. Требования к паролям определяются Политикой парольной защиты (см. раздел 8). Пароль к администраторской учетной записи должен храниться в запечатанном конверте в сейфе Начальника управления.

4.3.11. Администраторы сервера должны следовать принципу «наименьших привилегий». Не следует использовать администраторскую учетную запись, если можно выполнить задачу с применением непривилегированной учетной записи.

4.3.12. Удаленный привилегированный доступ, если это возможно, должен осуществляться с помощью протоколов SSH или IPSec[i] и технологии VPN[ii].

4.3.13. Серверы должны физически располагаться в помещении с ограниченным и контролируемым доступом. Размещать серверы в незащищенных помещениях запрещается.

4.3.14. Все связанные с безопасностью события критически важных серверов должны собираться системой мониторинга и храниться не менее 1 месяца. Ежедневные инкрементальные резервные копии должны храниться в течение 1 месяца. Ежемесячные полные резервные копии хранятся минимум 2 года.

4.3.15. Ответственные за администрирование и резервное копирование обязаны сообщать обо всех фактах, связанных с возможным нарушением информационной безопасности серверов.

4.3.16. В случае утраты или порчи серверного оборудования в Академии должно проводится служебное расследование силами сотрудников Управления информационных технологий.

5. ПОЛИТИКА БЕЗОПАСНОСТИ АКТИВНОГО СЕТЕВОГО ОБОРУДОВАНИЯ

5.1. Цель

5.1.1. Настоящая политика определяет минимально необходимые требования к настройке активного сетевого оборудования (маршрутизаторов и коммутаторов), имеющих соединение с сетью Академии и управляемых специалистами Академии.

5.1.2. Выполнение этой политики минимизирует вероятность нарушения режима информационной безопасности в отношении активного сетевого оборудования Академии.

5.2. Область действия

5.2.1. Политика затрагивает все сетевое оборудование, обеспечивающее соединение внешних сетей с корпоративной сетью Академии, а также сетевое оборудование во внутренней сети.

5.2.2. Политика обязательна для всех сотрудников Управления, выполняющих конфигурирование и администрирование активного сетевого оборудования.

5.3. Требования политики

5.3.1. На каждом активном сетевом устройстве должны быть выполнены следующие настройки:

5.3.1. На маршрутизаторе не должны создаваться никакие локальные учетные записи. Маршрутизаторы должны использовать протокол TACACS+[iii] для аутентификации сотрудников.

5.3.1. Enable-пароль на маршрутизаторе должен храниться в зашифрованном виде. Требования к Enable-паролям определяются Политикой парольной защиты. Enable-пароль маршрутизатора должен храниться в запечатанном конверте в сейфе Начальника управления.

5.3.1. Пароли, используемые производителями оборудования по умолчанию, должны быть изменены.

5.3.1. На маршрутизаторе должны быть отключены:

- Web-сервер маршрутизатора;
- Малые TCP-сервисы;
- Малые UDP-сервисы;
- Входящие пакеты с недействительными адресами.

5.3.1. Маршрутизатор должен быть включен в единую корпоративную систему управления сетью.

5.3.1. Маршрутизаторы должны использовать стандартизованный корпоративный протокол SNMP[iv].

5.3.2. За маршрутизатором закрепляется ответственный сотрудник Управления, выполняющий его обслуживание.

5.3.3. Текущие файлы конфигурации (настройки) маршрутизаторов должны подвергаться процедуре резервного копирования.

5.3.4. Сетевое оборудование должно быть промаркировано (например, наклейками на передней панели), так чтобы его можно было однозначно идентифицировать. Принцип маркирования должен быть унифицирован и донесен до сведения всех сотрудников, работающих с серверами.

5.3.5. В Академии должен поддерживаться реестр сетевого оборудования. По каждому сетевому оборудованию должна регистрироваться следующая минимальная информация:

- сетевой адрес;
- физическое местоположение (номер серверного помещения, номер стойки);
- производитель оборудования;
- ответственный за администрирование оборудования.

5.3.6. Информация об изменениях в конфигурации сетевого оборудования должна своевременно обновляться ответственными сотрудниками Управления. Логические и

физические связи сетевого оборудования должны быть отражены в общей схеме корпоративной сети.

5.3.7. В случае утраты или порчи активного сетевого оборудования в Академии должно проводится служебное расследование силами сотрудников Управления информационных технологий.

6. ПОЛИТИКА АУДИТА БЕЗОПАСНОСТИ

6.1. Цель

6.1.1. Настоящая политика определяет принципы внутреннего аудита информационной безопасности в Академии.

6.1.2. Выполнение этой политики позволяет оценивать эффективность существующей системы информационной безопасности Академии и своевременно реагировать на возникающие риски.

6.2. Область действия

6.2.1. Политика обязательна для сотрудников Управления информационных технологий, участвующих в проведении внутреннего аудит.

6.3. Требования политики

6.3.1. В целях совершенствования системы информационной безопасности Академии сотрудники Управления должны регулярно проводить внутренний аудит информационной безопасности.

6.3.2. Периодичность проведения внутреннего аудита – 1 раз в год. Аудит может проводиться раньше планового срока, в случае значительных изменений в корпоративной информационной системе Академии и в других случаях.

6.3.3. Аудит информационной безопасности должен включать анализ существующих рисков и угроз. По результатам анализа должны быть определены мероприятия по снижению выявленных рисков.

6.3.4. Аудит должен проводиться всесторонне, объективно и с использованием специализированных технических средств.

6.3.5. Отчет о результатах аудита безопасности готовится для руководства Академии и является конфиденциальной информацией.

7. ПОЛИТИКА КЛАССИФИКАЦИИ ДАННЫХ

7.1. Цель

7.1.1. Настоящая политика устанавливает принципы классификации данных и определяет требования к хранению и обработке в Академии информационной среде информации.

7.1.2. Выполнение этой политики минимизирует вероятность нарушения режима информационной безопасности при обработке конфиденциальных данных в информационных системах Академии.

7.2. Область действия

7.2.1. Политика обязательна для сотрудников Академии, обрабатывающих информацию в корпоративной информационной среде.

7.3. Требования политики

7.3.1. Вся информация в информационных системах делится на две категории – публичная и составляющая тайну (конфиденциальная).

7.3.2. При хранении и обработке информации, составляющей тайну, пользователи и сотрудники Академии обязаны строго соблюдать все требования и ограничения внутренних нормативных актов Академии.

7.3.3. Носители и резервные копии с конфиденциальной информацией должны быть промаркированы. Маркировка должна включать название отдела или управления, краткое описание хранимой информации и соответствующий гриф («Конфиденциально», «Коммерческая тайна» и т.п.).

7.3.4. Для конфиденциальной информации, обрабатываемой в корпоративной информационной среде Академии, должен быть установлен владелец (сотрудник Академии). Если другое не определено, то владельцем конфиденциальной информации является ее создатель.

7.3.5. Доступ сотрудникам Академии к конфиденциальной информации предоставляется только при условии и на основании разрешения, Ректора Академии и Первого проректора.

7.3.6. Распространение конфиденциальной информации за пределы Академии через информационные системы (электронная почта, сервисы сети Интернет и другие) в открытом виде запрещено.

7.3.7. Печать конфиденциальных документов на оборудовании Академии должна регистрироваться при наличии технической возможности.

7.3.8. Запрещается несанкционированное ксерокопирование бумажных носителей конфиденциальной информации и несанкционированная их передача факсимильным способом.

7.3.9. Пользователи обязаны сообщать обо всех известных им фактах, связанных с разглашением конфиденциальной информации Академии в Управление информационных технологий и Первому проректору Академии. По всем существенным фактам разглашения конфиденциальной информации должно проводится служебное расследование силами сотрудников Управления информационных технологий.

8. ПОЛИТИКА ПАРОЛЬНОЙ ЗАЩИТЫ

8.1. Цель

8.1.1. Политика устанавливает требования к созданию стойких к взлому паролей, принципы защиты таких паролей и периодичность их смены. Пароли являются первичным методом защиты доступа к информационным системам и разграничения прав пользователей.

8.1.2. Выполнение этой политики минимизирует вероятность нарушения режима информационной безопасности Академии при злоупотреблениях с паролями.

8.2. Область действия

8.2.1. Политика обязательна для сотрудников, имеющих доступ к любой корпоративной информационной системе, в том числе для сотрудников Академии.

8.3. Требования политики

8.3.1. Должны соблюдаться основные принципы выбора паролей:

- длина пароля должна быть не менее 8 символов;
- пароль не должен являться словом, которое можно найти в словаре;
- среди символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры или специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен быть тривиальным (например, a-111111, QWERTYUI или 12345678), не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, даты рождения, название Академии, клички домашних животных, а также номера автомобиля, телефона, паспорта, водительского удостоверения и т.д.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 позициях.

8.3.2. Все пароли уровня системы (в т.ч. администраторские пароли в приложениях) должны меняться не реже 1 раза в 3 месяца. Пользовательские пароли должны меняться не реже 1 раза в 4 месяца.

8.3.3. Максимальное количество попыток ввода пароля должно быть не больше 10. Превышение заданного числа попыток при неправильном вводе пароля должно вызывать блокировку учетной записи пользователя.

8.3.4. Все пароли на критичные элементы инфраструктуры (серверы, активное коммутационное оборудование) должны храниться в Управлении информационных технологиях.

8.3.5. Запрещается отправлять какие-либо пароли в сообщениях электронной почты или какими-то другими способами электронного обмена.

8.3.6. Запрещается сообщать кому-либо свои пароли по телефону и называть пароли в присутствии посторонних людей.

8.3.7. Запрещается использовать пароль в анкетных опросах и намекать на формат пароля.

8.3.8. Запрещается передавать пароли другим сотрудникам на время отпуска, командировки, болезни и т.п.

8.3.9. Запрещается хранить пароли на бумажных и других носителях.

8.3.10. Пользователи обязаны сообщать обо всех фактах, связанных с компрометацией их паролей (подозрениях на то, что пароль стал известен посторонним лицам) в Управление информационных технологий.

9. ПОЛИТИКА АНТИВИРУСНОЙ ЗАЩИТЫ

9.1. Цель

9.1.1. Настоящая политика определяет требования к антивирусной защите рабочих станций, ноутбуков и серверов корпоративной сети Академии.

9.1.2. Выполнение этой политики минимизирует вероятность заражения вирусами отдельных узлов сети и возникновения вирусных эпидемий.

9.2. Область действия

9.2.1. Политика обязательна для сотрудников Академии, в том числе для сотрудников всех его дочерних и зависимых обществ.

9.3. Требования политики

9.3.1. На серверах, рабочих станциях и ноутбуках Академии должно использоваться стандартное антивирусное ПО операционные системы Windows 10 Pro.

9.3.2. Базы вирусных сигнатур должны обновляться регулярно. В ИТ-подразделении назначается сотрудник, ответственный за обновление и администрирование антивирусного ПО.

9.3.3. Пользователям запрещается открывать файлы и выполнять вложения, полученные в сообщениях электронной почты от неизвестных или подозрительных отправителей. Подобные сообщения должны удаляться без возможности восстановления.

9.3.4. Запрещается загружать файлы или ПО с подозрительных или неизвестных узлов сети Интернет.

9.3.5. Конфигурация антивирусного ПО на рабочих станциях / ноутбуках должна обеспечивать автоматическую проверку подключаемых съемных носителей (CD/DVD-диски, USB-накопители и другие).

9.3.6. Пользователям запрещается отключать клиентское антивирусное ПО, при наличии у них достаточных полномочий (прав локального администратора).

9.3.7. Пользователи обязаны сообщать в Управление ИТ обо всех фактах, связанных с неработоспособностью и/или отключением антивирусного ПО.

10. ПОЛИТИКА РЕЗЕРВНОГО КОПИРОВАНИЯ И ВОССТАНОВЛЕНИЯ ДАННЫХ

10.1. Цель

10.1.1. Настоящая политика определяет требования к резервному копированию и восстановлению данных в Академии.

10.1.2. Выполнение этой политики минимизирует вероятность потери информации, обрабатываемой и хранимой на серверах, рабочих станциях и ноутбуках Академии.

10.2. Область действия

10.2.1. Политика обязательна для сотрудников Управление ИТ, выполняющих администрирование средств резервного копирования, в том числе для сотрудников ИТ-подразделений всех его дочерних и зависимых обществ.

10.3. Требования политики

10.3.1. Процедуры резервного копирования в Академии должны быть документированы (план резервного копирования). В плане резервного копирования должна быть указана: копируемая информация, порядок копирования, его периодичность и другая важная информация.

10.3.2. Резервные накопители должны быть промаркированы и храниться в защищенном месте (в сейфе и т.п.) вне помещения, где располагаются объекты резервного копирования (серверы и т.п.).

10.3.3. Процедура восстановления информации должна периодически тестироваться для проверки целостности резервных копий.

10.3.4. Процедура восстановления информации должна занимать минимальное время.

10.3.5. Сроки хранения резервных копий информации должны быть:

- для управленческой и финансовой информации – не менее 2 лет;
- для технической информации – не менее 1 года;
- для общей и неклассифицированной информации – не менее 3 месяцев.

10.3.6. Число сотрудников Академии, имеющих доступ к резервным накопителям, должно быть сведено к минимуму.

10.3.7. За каждой информационной системой (приложением) и/или устройством (сервер, рабочая станция) закрепляется сотрудник Управления ИТ, ответственный за резервное копирование информации.

11. ПОЛИТИКА ОРГАНИЗАЦИИ УДАЛЕННОГО ДОСТУПА

11.1. Цель

11.1.1. Политика определяет требования к процедурам предоставления сотрудникам Академии удаленного доступа к корпоративным информационным ресурсам.

11.1.2. Выполнение этой политики минимизирует вероятность нарушения режима информационной безопасности при удаленной работе пользователей с информационным системами Академии.

11.2. Область действия

11.2.1. Политика обязательна для сотрудников Академии, организующих и использующих удаленный доступ.

11.3. Требования политики

11.3.1. Удаленный доступ к информационным ресурсам Академии возможен только через защищенные сетевые соединения.

11.3.2. Для защиты соединения используются технология VPN, один из доступных протоколов: SSH, IPSec или SSL[v], однократные пароли или сертификаты корпоративной инфраструктуры открытых ключей.

11.3.3. Удаленный доступ должен предоставляться сотрудникам только в случае объективной необходимости.

11.3.4. Сотрудники, использующие удаленное подключение, должны гарантировать, что их компьютеры не подключены в то же самое время ни к каким другим сетям.

11.3.5. Сотрудникам запрещается передавать управление удаленным соединением другим лицам (пользователям), не являющимся сотрудниками Академии.

11.3.6. Запрещается использование удаленного доступа к корпоративной сети без предварительного согласования с Управление ИТ.

12. ПОЛИТИКА СОБЛЮДЕНИЯ ЛИЦЕНЗИРОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

12.1. Цель

12.1.1. Политика определяет принципы лицензирования используемого в Академии ПО.

12.1.2. Выполнение этой политики минимизирует риск возникновения претензий со стороны производителей ПО, которые могут негативно сказаться на функционировании информационной среды Академии.

12.2. Область действия

12.2.1. Политика обязательна для всех сотрудников Академии.

12.3. Требования политики

12.3.1. В Академии используется лицензионное программное обеспечение. Использование нелегальных копий коммерческого ПО недопустимо.

12.3.2. Для снижения стоимости лицензий в пересчете на одно рабочее место в Академии должны по возможности заключаться групповые соглашения с производителями ПО. Групповые соглашения должны предусматривать приобретение лицензий по льготным ценам.

12.3.3. Допускается использование бесплатного общедоступного ПО (ПО с открытым кодом) после его тестирования специалистами Управления ИТ.

12.3.4. Запрещается использовать лицензии на ПО в личных целях и устанавливать такое ПО на личных компьютерах, кроме случаев, когда это специально разрешено производителем ПО.

13. ПОЛИТИКА ПРЕДОСТАВЛЕНИЯ, ПРЕКРАЩЕНИЯ, ИЗМЕНЕНИЯ ПРАВ ДОСТУПА К СИСТЕМАМ АКАДЕМИИ

13.1. Цель

13.1.1. Настоящая политика определяет принципы доступа пользователей к информационным системам и ресурсам Академии.

13.1.2. Выполнение этой политики минимизирует вероятность несанкционированного доступа сотрудников к информационным системам и ресурсам Академии.

13.2. Область действия

13.2.1. Политика обязательна для сотрудников Академии, осуществляющих доступ к информационным системам и ресурсам, в том числе для сотрудников всех его дочерних и зависимых обществ.

13.3. Требования политики

13.3.1. За каждой информационной системой и информационным ресурсом закрепляется ответственный сотрудник – владелец информационной системы (ресурса).

13.3.2. Предоставление пользователям доступа к информационной системе (ресурсу) должно происходить по согласованию с владельцем этого ресурса. Владелец информационной системы (ресурса) отвечает за обоснованность предоставления прав доступа.

13.3.3. Предоставление, прекращение, изменение доступа к информационным системам (ресурсам) должно регистрироваться.

13.3.4. Доступ увольняемых сотрудников Академии к информационным системам (ресурсам) должен прекращаться сразу после завершения трудовых отношений с Академии.

13.3.5. Сотрудники Управления ИТ обязаны проводить периодический мониторинг соблюдения правил предоставления доступа.

13.3.6. Пользователям запрещено использовать чужие полномочия по доступу к информационным системам (ресурсам) и/или передавать кому-либо такие полномочия.

13.3.7. Пользователи обязаны сообщать обо всех фактах, связанных с нарушением правил доступа к информационным системам и ресурсам Академии в Управление ИТ.

13.3.8. Для каждой информационной системы (ресурса) Академии должны быть разработаны и поддерживаться в актуальном состоянии инструкции по работе пользователей и администраторов систем (ресурсов).

14. ПОЛИТИКА КОНТРОЛЯ ФИЗИЧЕСКОГО ДОСТУПА К ИТ-ИНФРАСТРУКТУРЕ

14.1. Цель

14.1.1. Политика определяет требования к физической безопасности объектов ИТ-инфраструктуры Академии.

14.1.2. Выполнение этой политики минимизирует вероятность несанкционированного физического доступа к объектам ИТ-инфраструктуры Академии, а так же вероятность их хищения и повреждения.

14.2. Область действия

14.2.1. Политика обязательна для всех сотрудников Управления ИТ.

14.3. Требования политики

14.3.1. Доступ к объектам ИТ-инфраструктуры (серверам, активному коммутационному оборудованию, устройствам хранения данных и др.) должен быть максимально ограничен для сотрудников, не работающих с данными объектами.

14.3.2. Объекты ИТ-инфраструктуры должны быть размещены в отдельных специализированных помещениях (серверных комнатах). Серверные помещения должны оборудоваться системами контроля доступа и, по возможности, системами видеонаблюдения. Объекты ИТ-инфраструктуры, расположенные вне серверных помещений, должны находиться в запирающихся шкафах.

14.3.3. За каждым элементом ИТ-инфраструктуры закрепляется ответственный сотрудник Управления ИТ.

14.3.4. Пользователи обязаны сообщать обо всех фактах, связанных с нарушением физической безопасности ИТ-инфраструктуры в Управлении ИТ.

15. ПОЛИТИКА РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

15.1. Цель

15.1.1. Политика определяет принципы реагирования на инциденты, связанные с информационной безопасностью, и проведения расследований.

15.1.2. Выполнение этой политики обеспечивает своевременное и эффективное реагирование в Академии на инциденты, связанные с информационной безопасностью.

15.2. Область действия

15.2.1. Политика обязательна для всех сотрудников Академии.

15.3. Требования политики

15.3.1. Для обнаружения инцидентов, связанных с информационной безопасностью, сотрудники Управления ИТ ведут систематический непрерывный мониторинг подсистем информационной безопасности Академии. Кроме того, выявление инцидентов происходит по обращениям пользователей Академии в Управление ИТ в рамках существующих бизнес-процессов.

15.3.2. Журналы подсистем ИБ должны просматриваться с периодичностью, достаточной для оперативного реагирования на инциденты. Кроме того, должен выполняться просмотр журналов в системах мониторинга в начале и конце каждого рабочего дня.

15.3.3. При обработке инцидента ИБ сотрудник Управления ИТ выполняет следующие шаги:

- классифицирует тип и приоритет инцидента;
- производит обязательное оповещение Начальника Управления ИТ, а также других сотрудников ДИТ и пользователей (при необходимости);
- определяет время начала и окончания, источник и характер атаки/инцидента;
- включает журналирование атаки/инцидента, если оно не ведется;
- всеми доступными средствами пытается прекратить атаку/инцидент или уменьшить ее последствия (в т.ч. выполняет изолирование поврежденных систем, участков сети);
- после завершения атаки/инцидента производит восстановление работоспособности сервисов самостоятельно или совместно с другими сотрудниками Управления ИТ.

15.3.4. Начальник Управления должен совместно с сотрудниками Управления готовить отчет по каждому существенному нарушению ИБ. Отчет о таких инцидентах направляется Первому проректору и после согласования Ректору.

15.3.5. После завершения расследования существенных инцидентов должен быть проведен анализ ситуации и подготовлены предложения по совершенствованию Политик безопасности Академии и используемых мер защиты.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Порядковый номер изменения	Номера листов (страниц)				Регистрационный номер изменения	Подпись лица, ответствен-ного за внесение изменений	Дата внесения изменения	Дата введения изменения в действие
	измененных	замененных	новых	аннулированных				
1	2	3	4	5	6	7	8	9

ЛИСТ ОЗНАКОМЛЕНИЯ

С документом ознакомлен:

№ п/п	Наименование должности	Фамилия И.О.	Подпись	Дата

[i] SSH – протокол защищенной передачи данных Secure Shell; IPSec – протокол защищенной передачи данных IP Security.

[ii] VPN – технология построения виртуальных частных сетей Virtual Private Network.

[iii] TACACS+ - протокол безопасного управления доступом.

[iv] SNMP – протокол управления и мониторинга сетевых устройств Simple Network Management Protocol.

[v] SSL – протокол защищенной передачи данных Secured Sockets Layer Level.