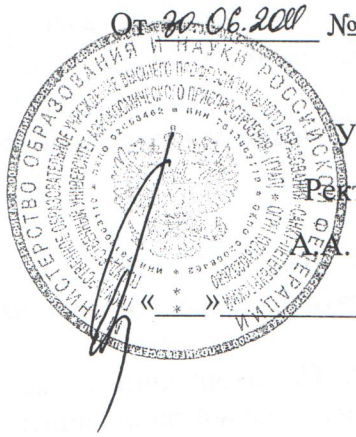
Приложение №2

к Приказу ГУАП

От 30.06.2011 № 01-125/11



Утверждаю

Ректор ГУАП

А.А. Оводенко

«__» _____2011 г.

ПОЛОЖЕНИЕ

Об обеспечении безопасности персональных данных в АИС ГУАП

1. Общие положения

1.1. Безопасность персональных данных в информационной системе АИС ГУАП обеспечивается в соответствии с законодательством Российской Федерации, государственными нормативно-методическими документами в области информационной безопасности и защиты персональных данных, учитывая общие принципы информационной безопасности, предусматриваемые международными и зарубежными национальными стандартами, в том числе ISO/IECIS 17799-2005, ISO/IEC 15408, ISO/IECIS 27001-2005.

1.2. Целью настоящего положения «Об обеспечении безопасности персональных данных в АИС ГУАП» (далее – Положение) является обеспечение безопасности персональных данных абитуриентов и студентов, обрабатываемых в информационной системе АИС ГУАП.

1.3. Обеспечение безопасности персональных данных включает в себя реализацию и поддержку процессов осознания необходимости обеспечения безопасности персональных данных, процессов руководства и управления безопасностью персональных данных. Процессы осознания имеют отношение как к руководству, так и к сотрудникам, работающих с персональными данными. Процессы осознания определяют ответственность сотрудников в части обеспечения безопасности персональных данных.

1.4. Обеспечение безопасности персональных данных в информационной системе АИС ГУАП обеспечивается за счет согласованного применения организационных, технических и программных мер и средств защиты на всех этапах подготовки, обработки, передачи и хранения информации.

1.5. Основные угрозы защищаемым ресурсам:

1.5.1. Основные источники угроз

1.5.1.1. Внешние:

1.5.1.1.1. Компьютерные злоумышленники, в том числе и бывшие работники ГУАП.

1.5.1.1.2. Абитуриенты, студенты ГУАП, в том числе и бывшие студенты.

1.5.1.2. Внутренние:

1.5.1.2.1. Специалисты по эксплуатации автоматизированных систем.

1.5.1.2.2. Разработчики автоматизированных систем.

1.5.1.2.3. Пользователи автоматизированных систем.

1.5.1.2.4. Работники ГУАП.

1.5.2. Основные угрозы

1.5.2.1. Внешние:

1.5.2.1.1. Атаки на информационные ресурсы

1.5.2.1.2. Атаки на аппаратно-программные и технические комплексы

1.5.2.2. Внутренние:

1.5.2.2.1. Невыполнение сотрудниками установленных правил и должностных инструкций

1.5.2.2.2. Несанкционированная деятельность работников, имеющих доступ к информационной системе, приводящих к изменению настроек оборудования, аппаратно-программных средств и комплексов, поражению рабочих станций вредоносными программами.

1.5.2.2.3. Деятельность, направленная на получение несанкционированного доступа к информационным ресурсам.

1.5.2.2.4. Несанкционированное использование информационных ресурсов (чтение, копирование, публикация).

1.6. Должен проводиться регулярный контроль целостности программного и аппаратного комплекса рабочих мест, где есть доступ к АИС ГУАП, а также серверной части.

1.7. Должен быть реализован «принцип эшелонированной защиты», который означает, что для реализации угрозы защищаемым ресурсам источник угрозы должен преодолеть несколько (более одного) уровней защиты.

1.8. Должна обеспечиваться регистрация и контроль действий, по крайней мере, всех администраторов и пользователей, обладающих максимальными полномочиями по доступу к информационным ресурсам, программным и техническим комплексам. Функция изменения результатов регистрации и контроля не должна быть доступна субъектам, за действами которого осуществляется контроль.

1.9. На всех автоматизированных рабочих местах и серверах должны применяться средства антивирусной защиты.

1.10. Должен быть исключён доступ посторонних лиц к рабочим местам сотрудников, имеющих доступ к информационной системе АИС ГУАП.

2. Персональные данные, обрабатываемые в информационной системе АИС ГУАП

2.1. Для организации поступления и учебного процесса в высшем учебном заведении абитуриенты и студенты обязаны предоставлять ряд персональных данных, в соответствии с законодательством Российской Федерации. Только следующие персональные данные обрабатываются в информационной системе АИС ГУАП:

№	Данные	Примечание	Категория
Общие данные			
1	ФИО		4
2	Пол		4
3	Дата рождения		3
Контактные данные			
4	Адрес места жительства		3
5	Почтовый индекс		3
6	Домашний телефон		3
7	Мобильный телефон		3
8	e-mail		3
Паспортные данные			
1	Серия		3
2	Номер		3
3	Кем выдан		3

4	Дата выдачи		3
5	Место рождения		3
6	Адрес регистрации		3
Карточка студента			
1	Код студента	Идентификатор	3
2	Статус		4
3	Номер студенческого билета		3
4	Форма обучения	Очная/Заочная/Очно-заочная/экстернат	4
5	Факультет		4
6	Группа		4
7	Курс		4
8	Специальность		4
9	Филиал		4
10	Форма возмещения	Контракт/Бюджет	4
11	Дата поступления		4
12	Есть ли льготы		3
13	Наличие договора		3
14	Номер договора		3
15	Слушатель		4
16	Приказы		4
Данные об успеваемости			
1	Оценки		4
2	Посещаемость		4
Договора			
1	Договора		3
Предыдущее образование			
1	Год окончания		3
2	Наименование		3
3	Адрес		3
4	Изучаемый иностранный язык		3
5	Тип документа		3
6	Номер документа		3

1.2. Обрабатываемые персональные данные в информационной системе АИС ГУАП подразделили на семь групп: Общие данные, Контактные данные,

Паспортные данные, Карточка студента, Данные об успеваемости, Договора, Предыдущее образование.

1.3. На территории ГУАП данные 4 категории считаются общедоступными.

1.4. Целью обработки персональных данных в информационной системе АИС ГУАП является организация процесса приема, обучения и отчисления в ГУАП.

1.5. Сроки обработки персональных данных студентов и абитуриентов в АИС ГУАП составляют:

1. Персональные данные не поступивших абитуриентов - 6 месяцев.
2. Персональные данные студентов отчисленных с 1 - 3 курсов – 15 лет.
3. Персональные данные остальных студентов и аспирантов – 20 лет.

По окончании срока хранения данные из информационной системы АИС ГУАП передаются на архивное хранение в архивный фонд личных дел ГУАП, а при необходимости статистической обработки обезличиваются.

3. Реализация ролевого доступа к персональным данным в системе АИС ГУАП

3.1. В системе реализован ролевой доступ к данным.

3.2. Право составления перечня ролей доступа в АИС ГУАП предоставляется проректору по административно-воспитательной работе и безопасности.

3.3. При необходимости создания новой роли, руководитель структурного подразделения направляет служебную записку, с указанием перечня групп персональных данных, к которым необходимо предоставить доступ новой роли, на имя проректора по административно-воспитательной работе и безопасности.

4. Должностная инструкция работника, имеющего доступ к АИС ГУАП

4.1. В информационной системе ГУАП находятся персональные данные студентов и абитуриентов.

4.2. Каждый сотрудник, имеющий доступ к персональным данным несет ответственность за неразглашение и безопасность персональных данных студентов и абитуриентов.

4.3. При обнаружении факта неправомерной подмены, удаления, разглашения и использования в собственных целях персональных данных работником университета, администрация ГУАП передаст информацию о совершении правонарушения в правоохранительные органы.

4.4. Каждый сотрудник, имеющий доступ к АИС ГУАП должен иметь свою учетную запись, защищенную паролем.

4.5. При входе в систему работник должен использовать только свой сертификат.

4.6. Сертификат действителен 1 год по умолчанию или на срок, оговоренный при подключении для конкретного пользователя.

4.7. Пароль необходимо менять ежегодно.

4.8. Пароль – это секретная информация, разглашение которой признается фактом разглашения персональных данных. Размещение пароля в открытом виде считается разглашением.

4.9. Если Ваш пароль узнал кто-либо, пароль необходимо сменить самостоятельно или обратившись к администратору.

4.10. При покидании своего рабочего места из информационной системы АИС ГУАП необходимо выйти.

4.11. Антивирус, установленный на компьютере с доступом в АИС ГУАП необходимо регулярно обновлять. Если обновления не происходит необходимо обратиться к администраторам.

4.12. При появлении предупреждений во время работы информационной системы АИС ГУАП внимательно его прочитайте и при необходимости обратитесь к администраторам.

4.13. Лица, не имеющий доступ к информационной системе АИС ГУАП, не должны иметь возможность доступа к ней или компьютеру, на котором установлен сертификат для доступа к системе. В случае если Вам стало известно о доступе посторонних лиц к информационной системе, незамедлительно сообщите об этом руководителю своего структурного подразделения и администраторам.

4.14. Администраторами системы АИС ГУАП являются назначенные работники подразделения ИИТО. К ним можно обратиться в ауд. 13-48 БМ, по телефонам 052, 494-70-52.

4.15. Нарушение настоящей должностной инструкции влечет ответственность в соответствии с действующим законодательством РФ.

5. Должностная инструкция руководителя подразделения, сотрудники которого имеют доступ в АИС ГУАП

5.1. Для подключения сотрудника Вашего структурного подразделения необходимо направить служебную записку на имя проректора по административно-воспитательной работе и безопасности с подробным описанием рабочего места, на котором необходимо настроить подключение (здание университета, аудитория телефон), и данными сотрудника, который будет иметь доступ к

информационной системе АИС ГУАП (должность, ФИО, и группы персональных данных, к которым необходим доступ для выполнения его должностных обязанностей). Образец служебной записки приведен в приложении А к настоящему Положению.

5.2. Полномочия и группы персональных данных, запрашиваемых при подключении должны быть минимально необходимыми для выполнения служебных обязанностей конкретного работника.

5.3. При необходимости расширения предоставляемого доступа сотруднику необходимо направить служебную записку на имя проректора по административно-воспитательной работе и безопасности.

5.4. Руководитель структурного подразделения должен следить за исполнением части 4 настоящего Положения сотрудниками, имеющими доступ к АИС ГУАП.

5.5. Лица, не имеющий доступ к информационной системе АИС ГУАП, не должны иметь возможность доступа к ней или компьютеру, на котором установлен сертификат для доступа к системе.

5.6. При увольнении или изменении должности работником структурного подразделения, имеющего доступ к информационной сети АИС ГУАП необходимо незамедлительно уведомить администраторов системы.

5.7. Администраторами системы АИС ГУАП являются назначенные работники подразделения ИИТО. К ним можно обратиться в ауд. 13-48 БМ, по телефонам 052, 494-70-52.

5.8. Нарушение настоящей должностной инструкции влечет ответственность в соответствии с действующим законодательством РФ.

6. Должностная инструкция администраторов АИС ГУАП

6.1. Администраторы информационной системы АИС ГУАП обязаны:

6.1.1. Оперативно реагировать на любые угрозы безопасности персональных данных студентов.

6.1.2. Проводить ознакомление с возможностями системы.

6.1.3. Разъяснять необходимость мер для обеспечения безопасности персональных данных.

6.1.4. Оперативно реагировать на обращения сотрудников университета по работе системы.

6.1.5. Вести журнал установленных сертификатов (Приложение Б к настоящему Положению).

6.1.6. Вести журнал учетных записей системы (Приложение В к настоящему Положению).

6.1.7. Вести автоматический журнал критических действий сотрудников, имеющих доступ к системе.

6.1.8. Не реже чем раз в неделю просматривать системные журналы.

6.1.9. При обнаружении несанкционированных действий со стороны пользователя уведомлять руководство в лице директора ИИТО и временно блокировать такого пользователя.

6.1.10. Нарушение настоящей должностной инструкции влечет ответственность в соответствии с действующим законодательством РФ.

Проректор
по административно-воспитательной
работе и безопасности И.А. Павлов

Директор ИИТО Е.А. Крук