	Министерство сельского хозяйства Российской Федерации
	ФГБОУ ВО Оренбургский ГАУ
	Политика безопасности в информационных системах

УТВЕРЖДЕНО
решением Ученого совета университета
«25» декабря 2015 г. протокол № 4
Председатель совета, и.о.ректора университета
_____ Г.В. Петрова

ПОДЛИННИК

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

Положение

Политика безопасности в информационных системах

СОГЛАСОВАНО:
Представитель руководства
университета по качеству
_____ Д.А. Сюсюра
«25» декабря 2015 г.

Оренбург, 2015

	Должность	***Фамилия/Подпись***	***Дата***
Согласовал	И.о.проректора по учебной работе	Маловский Н.А.	23.12.2015
	Начальник юридического отдела	Развозжаев Г.П.	23.12.2015
Проверил	Ведущий специалист УИКО	Бикмухаметова А.Х.	23.12.2015
Разработал	Директор ЦИТ	Солдатов В.Г.	22.12.2015
Версия: 01	Дата и время распечатки 23.12.2015 10:00		Стр. 1 из 13

Министерство сельского хозяйства
Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный аграрный университет»

П Р И К А З

г. Оренбург

11 января 2016 г. № 1

О введении в действие
политики безопасности
в информационных системах

На основании решения Ученого совета университета от 23 декабря 2015г. протокол № 4

ПРИКАЗЫВАЮ:

1. Ввести в действие положение «Политика безопасности в информационных системах».
2. Руководителям структурных подразделений обеспечить информирование сотрудников о введении в действие положения.
3. Директору ЦИТ разместить текст положения на официальном сайте университета.
4. И.о. проректора по информатизации обеспечить контроль за реализацией требований положения.

И.о. ректора университета,
профессор Г.В. Петрова

Верно: зав. канцелярией Р.С. Миронова

ПРЕДИСЛОВИЕ

Настоящая Политика безопасности в информационных системах ФГБОУ ВО Оренбургский ГАУ разработана в соответствии с требованиями МС ИСО 9001-2011 (ГОСТ ISO 9001:2008) и федерального закона №149-ФЗ 27.07.2006 г. «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями).

Введено в действие приказом и.о. ректора Университета № 1 от «11» января 2016 г. на основании решения Ученого совета № 4 от «22» декабря 2015 г

1 ОБЛАСТЬ ПРИМЕНЕНИЯ И СФЕРА ДЕЙСТВИЯ

Политика безопасности в информационных системах (далее – Политика) определяет общие правила обеспечения информационной безопасности в информационных системах (далее – Системы) ФГБОУ ВО Оренбургский ГАУ (далее – Университет). Процедуры и правила использования тех или иных Систем могут быть установлены дополнительными локальными нормативными документами.

Политика разработана на основании руководящих принципов и рекомендаций международного стандарта ISO/IEC 17799-1.

Требования Политики обязательны к исполнению для всех сотрудников Университета, использующих информационные системы.

2 НОРМАТИВНЫЕ ССЫЛКИ

Настоящее Положение разработано с учётом требований следующих нормативно-правовых документов:

- Федерального закона «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ (с изменениями и дополнениями);
- Федерального закона «О персональных данных» от 27 июля 2006г. № 152-ФЗ (с изменениями и дополнениями);
- Федерального закона «О коммерческой тайне» от 29 июля 2004г. № 98-ФЗ (с изменениями и дополнениями);
- ГОСТ ISO 9001-2011 (ISO 9001:2008) «Системы менеджмента качества. Требования»;
- ГОСТ ISO 9000-2011 (ISO 9000:2005) «Системы менеджмента качества. Основные положения и словарь»;
- Устава Университета;
- Политики и Целей в области качества;
- Правил внутреннего трудового распорядка Университета;
- Кодекса профессиональной этики и служебного поведения сотрудников.

3 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем Положении использованы термины и определения в соответствии с ГОСТ ISO 9000-2011 (ISO 9000:2005), а также связанные со спецификой реализуемого процесса.

Администратор Системы – привилегированный пользователь, выполняющий функции сопровождения и администрирования Системы;

Владелец информационного ресурса – структурное подразделение Университета, уполномоченное к управлению содержанием информационного ресурса и несущее ответственность за обеспечение его безопасности в части авторизации прав доступа;
Доменная учетная запись – учетная запись, от имени которой субъект, осуществляет работу в Системе;
Доменное имя – обозначение символами, предназначенное для идентификации информационного ресурса пользователя;
Доступность – возможность получения и использования информации и смежным ресурсов авторизованных пользователей тогда, когда им это необходимо;
Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
Информационные ресурсы – различные виды университетской информации (образовательной, финансово-аналитической, кадрово-управленческой и пр.) на следующих фазах её жизненного цикла: генерация (создание), обработка, хранение, передача, уничтожение;
Конфиденциальность – обеспечение доступа к информации только для авторизованных пользователей;
Пользователь – субъект, осуществляющий работу в Системе;
Целостность – обеспечение полноты и точности информации и методов её обработки.

4 ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В Положении использованы следующие обозначения и сокращения:
ИСПД и БД – информационные системы передачи данных и баз данных;
ПДн – персональные данные;
Политика – настоящая политика безопасности в информационных системах
СУБД – система управления базами данных;
ТК РФ – трудовой кодекс Российской Федерации;
УЗ – учетная запись;
Университет – федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный аграрный университет»;
УФУ – учетно-финансовое управление;
ЦИТ – центр информационных технологий.

5 ОБЩИЕ ПОЛОЖЕНИЯ

Информация может быть представлена в различных формах, сохранена на персональных компьютерах или серверах, передана по сети, распечатана или переписана на бумагу, пересказана собеседнику.

Информационная безопасность предусматривает защиту всех форм и средств обработки информации в целях гарантированного обеспечения её целостности, конфиденциальности и доступности.

5.1 Цель и задачи Политики

5.1.1 Информация и Системы являются одним из жизненно важных ресурсов Университета, обеспечивающих его эффективную работу. Несанкционированный доступ и несанкционированное использование Систем и информации может явиться причиной материального ущерба для Университета.

5.1.2 Цели и задачи Политики заключаются в следующем:

- обеспечить целостность, конфиденциальность и доступность информации и Систем Университета;
- обеспечить непрерывность образования и минимизировать ущерб Университета путём предотвращения возможных инцидентов информационной безопасности;
- обеспечить соответствие мер, принимаемых в области защиты информации Университета;
- предоставить сотрудникам Университета рекомендации и содействие в области защиты информации.

5.2 Разработка, внедрение и пересмотр Политики

5.2.1 Ответственным за разработку, внедрение, документирование, пересмотр и изменение Политики является Центр информационных технологий Университета.

5.2.2. Эффективность действия Политики ежегодно оценивается Проректором по информатизации по характеристикам: доступность информации, обеспечение конфиденциальности, соответствие внешним требованиям к защите информации.

5.2.3. Структурные подразделения - владельцы информационных ресурсов могут устанавливать дополнительные процедуры обеспечения безопасности, регулирующие предоставление прав доступа к вверенным им ресурсам. Эти процедуры могут быть более детализированы, предусматривать дополнительные ограничения, но не могут противоречить настоящей Политике.

5.2.4. Сотрудники Университета должны сообщать в ЦИТ о ставших им известными недостатках в системе защиты информации, нарушениях требований настоящей Политики и других угрозах информационной безопасности.

5.2.5. Положения Политики подлежат пересмотру в случае изменения организационной или технологической инфраструктуры Университета, серьёзных инцидентов безопасности, выявления новых угроз, уязвимостей, наличия иных значимых изменений.

5.3. Логический доступ к информационным ресурсам

5.3.1. Университетские информационные ресурсы могут использоваться сотрудниками Университета только в служебных целях. Вся информация, хранящаяся в Системах и предоставляемая Системами, является конфиденциальной (*в т.ч. персональные данные и др.*), за исключением информации, доступ к которой не ограничивается в соответствии с законодательством Российской Федерации и локальными нормативными документами Университета (*сведения об образовательной организации и др.*).

5.3.2 Необходимым условием доступа к информационным ресурсам и Системам Университета является ознакомление сотрудника Университета с данной Политикой.

5.3.3. Сотрудникам Университета предоставляются права доступа к информационным ресурсам в соответствии с их служебными обязанностями. Каждому пользователю Системы администратор ЦИТ назначает уникальный идентификатор – Доменную УЗ.

5.3.4. При обработке критичной информации должна обеспечиваться возможность определения авторства (протоколирование) каждой выполненной операции на основе идентификаторов пользователей.

5.3.5. Запрещается использование ресурсов, к которым у сотрудника нет прав доступа. Возможность доступа пользователя к ресурсам, не предусмотренным его служебными обязанностями, не означает получения права на их использование.

5.3.6. Сотрудникам запрещается работа в Системах под именами других пользователей и с использованием чужих паролей доступа, запрещается передача прав доступа к информационным ресурсам, а также несанкционированное копирование, изменение, уничтожение данных, хранящихся в Системах Университета.

5.3.7. Основным средством доступа к информационным ресурсам Университета является персональный компьютер. За каждым компьютером закрепляется ответственный пользователь, определяемый руководителем структурного подразделения до установки/настройки компьютера сотрудниками ЦИТ.

5.3.8. Ответственный пользователь не должен допускать работы других пользователей на своем персональном компьютере под своей доменной УЗ, такая работа возможна только в случае служебной необходимости с разрешения руководителя структурного подразделения.

5.3.9. При передаче персонального компьютера другому пользователю локальный диск компьютера может быть переформатирован сотрудниками ЦИТ по усмотрению руководителя структурного подразделения, в котором этот компьютер эксплуатировался. Форматирование диска в этом случае должно производиться по согласованию и под контролем руководителя данного структурного подразделения с составлением акта (в свободной форме).

5.3.10. При подключении компьютера сотрудниками ЦИТ устанавливается стандартная конфигурация программного обеспечения. Стандартная конфигурация рабочего места пользователя включает в себя операционную систему Microsoft Windows, средства Microsoft Office, антивирусное программное обеспечение; либо операционную систему Ubintu Linux (или аналог) и все сопутствующее ПО.

5.3.11. Пользователям запрещается:

- самостоятельно изменять конфигурацию программных и аппаратных средств персонального компьютера, осуществлять установку и удаление прикладных программ, изменять системные параметры, уничтожать или добавлять файлы в системные директории;

- изменять установленное администратором состояние разделения дисковых ресурсов компьютера, т.е. создавать или удалять разделяемые ресурсы;

- изменять любые настройки доступа к сети.

5.3.12. Ответственный Пользователь несёт ответственность за наличие/отсутствие на локальном диске вверенного компьютера посторонних программ, установленных без участия специалистов ЦИТ.

5.3.13. Запрещается для хранения конфиденциальной информации использовать общедоступные сетевые диски.

5.3.14. Для пересылки электронных документов, содержащих закрытую информацию структурного подразделения, внутри Университета Пользователь обязан использовать систему электронной почты, рекомендованную ЦИТ.

5.3.15. При использовании портативных компьютеров (ноутбуков и т.п.) за пределами территории Университета, ответственный пользователь несёт ответственность за безопасность и сохранность портативного компьютера, а также за конфиденциальность информации, обрабатываемой на нём.

5.3.16. При удаленном подключении к информационным ресурсам Университета, ЦИТ должна быть обеспечена достаточная защита, направленная на минимизацию рисков кражи информации, несанкционированного раскрытия информации, несанкционированного удалённого доступа к системам Университета, злоупотребления предоставленными ресурсами.

5.4. Использование носителей компьютерной информации

5.4.1. При необходимости записи конфиденциальной информации на флэш-карты, лазерные диски или другие носители сотрудник должен получить соответствующее разрешение руководителя структурного подразделения, в котором он работает, если иное не определено его служебными обязанностями.

5.4.2. Пользователь обязан своевременно уничтожать утратившие актуальность копии документов, содержащих конфиденциальную информацию. Окончательное уничтожение информации на магнитных носителях выполняется путём полного форматирования последних.

5.4.3. Использование флэш-карт или других магнитных носителей информации возможно только после обязательной проверки их на наличие вирусов. В случае обнаружения вирусов на магнитном носителе или в памяти компьютера работа с данными устройствами прекращается до уничтожения вирусов. Университетские переносные магнитные носители подлежат обязательному учёту.

5.5. Пароли

5.5.1. Доступ к использованию ресурсов информационных систем предоставляется после ознакомления с настоящей Политикой.

5.5.2. В момент предоставления сотруднику прав доступа к Системе администратор сообщает Пользователю логин и пароль. Пользователь обязан обеспечить конфиденциальность своих личных паролей. Запрещается разглашать и передавать свои пароли другим сотрудникам, а также размещать пароль в электронном виде на магнитных носителях.

5.5.3. Пользователю рекомендуется регулярно (не реже одного раза в три месяца) менять свои пароли. Смена пароля в обязательном порядке производится при нарушении его конфиденциальности или по указанию администратора соответствующей Системы.

5.5.4. В случае, если Пользователь самостоятельно выбирает последовательность символов для пароля, ему рекомендуется использовать в пароле сочетание букв верхнего и нижнего регистров, цифр и знаков пунктуации длиной не менее 7 (семи) знаков.

5.5.5. В качестве личного пароля сотруднику Университета, осуществляющему работу с конфиденциальной информацией, запрещается использовать:

- последовательности символов, состоящие из одних цифр (в том числе даты, номера телефонов и т.д.);

- последовательности повторяющихся букв;

- подряд идущие в раскладке клавиатуры или в алфавите символы;

- имена и фамилии;

- имя пользователя в Системе (идентификатор) и общеупотребительные сокращения (ЭВМ, ЛВС, user, admin и т.д.);

- осмысленные английские или русские слова;

- ассоциированную с сотрудником информацию, которую легко узнать (адрес, марка автомобиля и т.д.).

5.5.6. В случае, если Пользователь забыл свой пароль и не может получить доступ к информационным ресурсам, руководитель данного структурного подразделения должен обратиться к администратору соответствующей Системы (ЦИТ).

5.5.7. Пользователю разрешается использовать один и тот же пароль для входа в сеть, в систему электронной почты, другие Системы.

5.5.8. Пароли, установленные по умолчанию в приложениях и операционных системах (во время инсталляции), подлежат немедленной замене после начала использования системы (приложения).

5.6. Электронное архивирование информации

5.6.1 Электронное архивирование информации должно обеспечивать сохранение юридически значимой и другой представляющей ценность для Университета информации, возможность разрешения спорных ситуаций и проведения расследований в случаях нарушений информационной безопасности.

5.6.2. Электронному архивированию подлежат:

- электронные документы; электронные образы бумажных документов; электронные протоколы (регистрационные журналы, log-файлы и т.п.) работы Систем;

- открытые ключи электронной цифровой подписи;

- любая другая информация в электронном виде, для которой определена необходимость архивирования.

5.6.3. Электронные архивы должны удовлетворять следующим требованиям:

- архив не доступен для записи или удаления информации любым лицом, кроме ответственного за ведение архива, определенного руководителем соответствующего структурного подразделения;

- документы в архиве хранятся со всеми возможными подтверждениями их подлинности, в частности, с электронной цифровой подписью (для документов, которые были подписаны электронной цифровой подписью);

- архив надёжно защищён от утраты и уничтожения (дублирование, хранение в сейфах, несгораемых шкафах, выбор носителей соответствующей надежности).

5.7. Обеспечение доступности информационных систем

5.7.1. Для Систем, обрабатывающих критичную информацию, должно обеспечиваться сохранение (восстановление) их работоспособности при утере, уничтожении, несанкционированной модификации данных, программного обеспечения, выходе из строя оборудования и т.п.

5.7.2. Сопровождение работы аппаратного и программного обеспечения предусматривает:

- контроль за несанкционированной установкой аппаратного или программного обеспечения;

- контроль за несанкционированным изменением программ и прав доступа к ним;

- хранение эталонных копий программ, исходных текстов программного обеспечения, в том числе и предыдущих версий, в специальных библиотеках программного обеспечения;

- разделение технологических процессов разработки, тестирования, переноса в промышленную среду и эксплуатации программного обеспечения;

- контроль и документирование любых изменений аппаратной и программной частей Систем, отражение изменений в прикладном программном обеспечении в номере версии, системной документации и документации пользователей.

5.7.3. Резервное копирование информации должно удовлетворять следующим требованиям:

- обеспечивать возможность восстановления программ и данных в случае возникновения аварийной ситуации;

- копии программного обеспечения и данных должны располагаться в безопасном месте, защищенном от пожаров и иных угроз;

- периодически должна проверяться возможность восстановления информации с копий.

5.7.4. Периодичность резервного копирования должна позволять восстановить работу Систем без существенных потерь для Университета в кратчайшее время. Периодичность резервного копирования общеуниверситетских систем определяется директором ЦИТ.

5.7.5. Минимально необходимый и достаточный объём копируемой информации, вместе с точными и полными перечнями резервных копий и документированными процедурами восстановления, должен храниться удаленно и на достаточном расстоянии с целью предотвращения ущерба в случае аварии на основной серверной площадке.

5.7.6. Резервированию подлежит: серверное и сетевое оборудование; программное обеспечение; каналы связи; информационные базы данных.

5.8. Антивирусная защита

5.8.1. Антивирусная защита информационных ресурсов Университета осуществляется централизованно усилиями ЦИТ и должна обеспечивать контроль:
- информации, входящей из глобальных сетей во внутреннюю сеть Университета;
- информации, хранящейся на файловых серверах Университета;
- информации, хранящейся на персональных компьютерах сотрудников Университета.

5.8.2. На всех файловых серверах Университета должно быть установлено антивирусное программное обеспечение с проведением ежедневной проверки на вирусы всех программ и файлов данных на файловых серверах.
5.8.3. Рабочие станции пользователей должны иметь резидентные антивирусные программы, обеспечивающие проверку на вирусы всех файлов при их загрузке в компьютер, а также антивирусные сканеры для полной проверки жёстких дисков.
5.8.4. Антивирусные программы и базы вирусных сигнатур должны централизованно обновляться.
5.8.5. Пользователи обязаны информировать Системного администратора о любом обнаруженном вирусе, изменении конфигурации, необычном поведении компьютера или программы.
5.8.6. При обнаружении вируса должны быть приняты следующие меры:

- Системный администратор предупреждает всех пользователей, имеющих доступ к программам и данным, в которых обнаружен вирус, о возможном заражении их компьютеров;
- любой компьютер, который подозревается в заражении вирусом, немедленно отключается от сети;
- зараженный компьютер не подключается к сети до тех пор, пока Системные администраторы не удостоверятся в успешном результате лечения (удалении) вируса;
- если вирус удалить не удается, все программы в компьютере удаляются, включая, при необходимости, операционную систему, жесткий диск форматируется;
- удалённые программы повторно устанавливаются из надежных источников и повторно проверяются на наличие вирусов;
- проводится анализ причин заражения вирусом и принимаются необходимые меры безопасности.

5.9 Требования к защите помещений

5.9.1. Помещения Университета, в которых располагаются средства вычислительной техники, должны оборудоваться охранно-пожарной сигнализацией, а при необходимости средствами инженерной защиты и контроля доступа.

5.9.2. Помещения с серверным оборудованием, на котором обрабатывается критичная информация, должны быть оборудованы достаточными средствами кондиционирования, измерения и контроля температуры и влажности воздуха, средствами охранной сигнализации, системой контроля доступа и автоматизированной системой пожаротушения, системой контроля состояния электроснабжения, при необходимости – средствами видеонаблюдения. Доступ в эти помещения предоставляется строго определенным лицам в соответствии с утвержденными служебными обязанностями, время входа и выхода из помещения должно фиксироваться в специальной базе данных.

5.9.3. Руководители структурных подразделений Университета должны обеспечивать соблюдение соответствующего режима доступа в помещения с серверной вычислительной техникой, исключающего несанкционированное нахождение в них и несанкционированное использование вычислительной техники.

5.10 Функции по обеспечению информационной безопасности

5.10.1. Ведущую роль в разработке стратегии информационной безопасности Университета играет Центр информационных технологий, который:

- готовит для руководства Университета предложения по формированию бюджета, направленного на обеспечение информационной безопасности;
- разрабатывает политики и процедуры информационной безопасности;
- разрабатывает технические, организационные и административные планы обеспечения реализации политики информационной безопасности;
- обеспечивает штатное функционирование комплекса средств информационной безопасности Университета.
- обеспечивает мониторинг функционирования системы управления информационной безопасности Университета;
- проводит консультацию сотрудников Университета в области информационной безопасности;
- оценивает риски информационной безопасности, контролирует действия пользователей;
- обеспечивает выбор средств и механизмов контроля, управления и обеспечения информационной безопасности Университета;
- проводит расследование событий, связанных с нарушениями информационной безопасности (инцидентов безопасности);
- обеспечивает исполнение требований информационной безопасности, изложенных в настоящей Политике и других локальных нормативных документах Университета.

5.10.2. Сотрудники Университета в рамках обеспечения информационной безопасности:

- выполняют требования информационной безопасности, изложенные в настоящей Политике и других локальных нормативных документах Университета, в том числе связанных с защитой персональных данных;
- способствуют выполнению требований информационной безопасности третьими лицами, с которыми они контактируют в рамках своих должностных обязанностей, в том числе путём указания требований в контрактах/ соглашениях/ договорах с третьими лицами.

6 ОТВЕТСТВЕННОСТЬ И ПОЛНОМОЧИЯ

6.1. ЦИТ несёт первичную ответственность за состояние информационной безопасности в Университете.

6.2. Руководители структурных подразделений, использующих в своей работе информационные Системы, несут ответственность за нарушение подчиненными сотрудниками требований настоящей Политики.

6.3. Сотрудник Университета несёт персональную ответственность за все действия, выполняемые им в Системах Университета в соответствии с внутренними нормативными документами Университета и законодательством РФ.

6.4. Мера и степень ответственности определяются законодательством РФ.