УТВЕРЖДАЮ
И.о. министра Министерства по
внешнеэкономическим связям и туризму
Республики Тыва
_____ /Р.М. Самбу-Хоо
«06» августа 2021 г.

ИНСТРУКЦИЯ
ответственного за защиту информации в государственной информационной системе Министерства по внешнеэкономическим связям и туризму Республики Тыва

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция разработана в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11.02.2013 г. № 17.

1.2. Настоящая инструкция определяет задачи, функции, обязанности, ответственность и права ответственного за защиту информации в государственной информационной системе Министерства по внешнеэкономическим связям и туризму Республики Тыва.

1.3. Ответственный за защиту информации в пределах своих функциональных обязанностей обеспечивает безопасность информации обрабатываемой, передаваемой и хранимой в государственной информационной системе Министерства по внешнеэкономическим связям и туризму Республики Тыва.

2. ОСНОВНЫЕ ЗАДАЧИ И ФУНКЦИИ ОТВЕТСТВЕННОГО ЗА ЗАЩИТУ ИНФОРМАЦИИ

2.1. Основными задачами ответственного за защиту информации являются:

– организация эксплуатации технических и программных средств защиты информации, в том числе персональных данных;

– текущий контроль работы средств и систем защиты информации;

– организация и контроль резервного копирования информации, в том числе персональных данных.

2.2. Ответственный за информационную безопасность выполняет следующие основные функции по:

– разработке инструкций по информационной безопасности;

– обучению работников Министерства по внешнеэкономическим связям и туризму Республики Тыва правилам безопасной обработки информации и правилам работы со средствами защиты информации;

– организации антивирусного контроля магнитных носителей информации и файлов электронной почты, поступающих в Министерства по внешнеэкономическим связям и туризму Республики Тыва;

– текущему контролю работоспособности и эффективности функционирования эксплуатируемых программных и технических средств защиты информации, в том числе персональных данных;

– контролю за санкционированным изменением программного обеспечения, заменой и ремонтом средств вычислительной техники;

– контролю пользования Интернетом.

3. Обязанности ответственного за информационную безопасность

3.1. Обеспечивать функционирование и поддерживать работоспособность средств и систем защиты информации, в том числе персональных данных, в пределах, возложенных на него обязанностей.

Немедленно докладывать руководителям органов Администрации о выявленных нарушениях и несанкционированных действиях пользователей и работников, а также принимать необходимые меры по устранению нарушений.

3.2. Совместно с администратором сети, администраторами информационных систем персональных данных, программистами органов Администрации, ЗАТО Сибирский принимать меры по восстановлению работоспособности средств и систем защиты информации.

3.3. Проводить инструктаж работников и пользователей средств вычислительной техники по правилам работы с используемыми средствами и системами защиты информации.

3.4. Контролировать создание и удаление учетных записей пользователей, формирование паролей для новых пользователей.

3.5. Отслеживать работу антивирусных программ, в том числе результаты еженедельной полной проверки компьютеров, на наличие вирусов пользователями.

3.6. Контролировать регулярность резервного копирования данных, в том числе персональных данных. Оказывать помощь в восстановлении потерянных или поврежденных данных.

3.7. По запросам Главы Администрации, руководителей органов Администрации, ЗАТО Сибирский готовить статистическую информацию по пользованию Интернетом работниками Администрации, ЗАТО Сибирский и органов Администрации, ЗАТО Сибирский.

3.8. Вести учет пользователей Администрации, ЗАТО Сибирский сети Интернет. В случае необходимости лимитировать время работы и объем скачиваемой информации.

3.9. Готовить предложения по совершенствованию используемых систем защиты информации и отдельных их компонентов.

4. Права ответственного за информационную безопасность

4.1. Ответственный за информационную безопасность Администрации, ЗАТО Сибирский вправе требовать от работников и пользователей компьютерной техники Администрации, ЗАТО Сибирский и органов Администрации ЗАТО Сибирский безусловного соблюдения установленной технологии и выполнения инструкций по обеспечению безопасности и защиты информации, в том числе персональных данных.

5. Ответственность ответственного за информационную безопасность

5.1. На ответственного за информационную безопасность возлагается персональная ответственность за качество проводимых им работ по обеспечению защиты информации в соответствии с функциональными обязанностями, определенными в настоящем Положении.

3. ОБЯЗАННОСТИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

Администратор безопасности обязан:

– разработать и исполнять утверждённый план проведения мониторинга информационной безопасности ИС от несанкционированного распространения и доступа, искажения и утраты информации;

– вести разъяснительную работу с сотрудниками по вопросам информационной безопасности;

– обеспечить полное стирание защищаемой информации с электронных носителей в случаях их передачи для обслуживания или ремонта;

– обеспечить уничтожение защищаемой информации со съёмных носителей, не предназначенных для дальнейшего использования, методом многократной перезаписи без возможности восстановления;

– проверять электронный журнал обращений к РИС;

– контролировать надлежащее функционирование программных и технических СЗИ, входящих в состав РИС, во всех режимах работы, а именно:

1) использование только лицензионного (сертифицированного) программного обеспечения;

2) использование только сертифицированных средств защиты информации;

3) соблюдение условий использования и правильность конфигурирования (настройки) средств защиты информации.

В обязанности Администратора безопасности входит:

– проведение разбирательств и составление заключений по фактам несоблюдения условий хранения носителей ЗИ, использования средств защиты информации;

– уничтожение пришедших в негодность машинных носителей ЗИ.

4. Мониторинг

Мониторинг парольной защиты и контроль надёжности пользовательских паролей предусматривают:

– установление сроков действия паролей – минимального и максимального;

– периодическую проверку пользовательских паролей на количество символов и очевидность с целью выявления слабых паролей.

Мониторинг целостности программного обеспечения включает следующие действия:

– проверка контрольных сумм и цифровых подписей каталогов и файлов сертифицированных программных средств защиты при загрузке операционной системы;

– обнаружение дубликатов идентификаторов пользователей;

– восстановление системных файлов администраторами систем с резервных копий при несовпадении контрольных сумм.

Антивирусный контроль: администратор безопасности контролирует регулярность обновления антивирусных баз на серверах.

5. Системный аудит

Системный аудит производится ежеквартально и в особых ситуациях. Он включает проведение обзоров безопасности, тестирование РИС, контроль внесенных изменений в системное программное обеспечение.

Обзоры безопасности проводятся с целью проверки текущего уровня безопасности РИС. Обзоры безопасности имеют целью выявление всех несоответствий между текущим состоянием РИС и состоянием, соответствующем специально составленному списку для проверки.

Обзоры безопасности содержат:

– отчёты о безопасности пользовательских ресурсов, включающие наличие повторяющихся пользовательских имён и идентификаторов, неправильных форматов регистрационных записей, пользователей без пароля, неправильной установки домашних каталогов пользователей и уязвимостей пользовательских окружений;

– проверку правомочности предоставления прав доступа пользователей к сетевым ресурсам;

– проверку содержимого файлов конфигурации на соответствие списку для проверки;

– обнаружение изменений системных файлов со времени проведения последней проверки (контроль целостности системных файлов);

– проверку прав доступа и других атрибутов системных файлов;

– проверку правильности настройки механизмов аутентификации и авторизации сетевых сервисов;

– проверку корректности конфигурации системных и активных сетевых устройств (мостов, маршрутизаторов, концентраторов и сетевых экранов).

Активное тестирование надёжности механизмов контроля доступа производится путём осуществления попыток проникновения в систему (с помощью автоматического инструментария или вручную).

Пассивное тестирование механизмов контроля доступа осуществляется путём анализа конфигурационных файлов системы. Информация об известных уязвимостях извлекается из документации и внешних источников. Затем осуществляется проверка конфигурации системы с целью выявления опасных состояний системы, т.е. таких состояний, в которых могут проявлять себя известные уязвимости.

6. Анализ инцидентов

Если администратор безопасности подозревает или получил сообщение о том, что система подвергается атаке или уже была скомпрометирована, то он должен установить:

– факт попытки несанкционированного доступа (НСД);

– продолжается ли НСД в настоящий момент;

– кто является источником НСД;

– что является объектом НСД;

– когда происходила попытка НСД;

– как и при каких обстоятельствах была предпринята попытка НСД;

– точка входа нарушителя в систему;

– была ли попытка НСД успешной;

– определить системные ресурсы, безопасность которых была нарушена;

– какова мотивация попытки НСД.

Для выявления попытки НСД необходимо установить, какие пользователи в настоящее время работают в системе, на каких рабочих станциях. Выявить подозрительную активность пользователей, проверить, что все пользователи вошли в систему со своих рабочих мест, и никто из них не работает в системе необычно долго. Кроме того, необходимо проверить, что никто из пользователей не выполняет подозрительных программ и программ, не относящихся к его области деятельности.

При анализе системных журналов администратору безопасности необходимо произвести следующие действия:

– проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД, включая вход в систему пользователей, которые должны бы были отсутствовать в этот период времени, входы в систему из неожиданных мест, в необычное время и на короткий период времени;

– проверить, не уничтожен ли системный журнал и нет ли в нем пробелов;

– просмотреть списки команд, выполненных пользователями в рассматриваемый

период времени;

– проверить наличие мест в системных журналах, которые выглядят необычно;

– выявить попытки получить полномочия суперпользователя или другого привилегированного пользователя;

– выявить наличие неудачных попыток входа в систему.

В ходе анализа журналов активного сетевого оборудования (мостов, переключателей, маршрутизаторов, шлюзов) необходимо:

– проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД;

– проверить, не уничтожен ли системный журнал и нет ли в нем пробелов;

– проверить наличие мест в журналах, которые выглядят необычно;

– выявить попытки изменения таблиц маршрутизации и адресных таблиц;

– проверить конфигурацию сетевых устройств с целью определения возможности нахождения в системе программы, просматривающей весь сетевой трафик.

Для обнаружения в системе следов, оставленных злоумышленником, в виде файлов, вирусов, троянских программ, изменения системной конфигурации необходимо:

– составить базовую схему того, как обычно выглядит система;

– провести поиск подозрительных файлов и каталогов, которые могли быть использованы злоумышленниками;

– проверить содержимое системных файлов, которые могли быть изменены злоумышленниками;

– проверить целостность системных программ;

– проверить систему аутентификации и авторизации.

В случае заражения значительного количества АРМ после устранения его последствий проводится системный аудит.

7. Контроль резервного копирования и восстановления информации

На этапе исполнения администраторами информационных систем «Плана резервного копирования», Администратор безопасности обязан контролировать сроки создания копий, анализировать состояние носителей (количество сбойных участков, объем свободного места) и незамедлительно докладывать руководству обо всех произошедших или ожидаемых отклонениях от плана.

Администратор безопасности согласовывает, разработанный системными администраторами, «Регламент восстановления повреждённых или утраченных данных информационной системы».

8. Шифрование данных

При необходимости шифрования данных, обрабатываемых с помощью технических средств РИС, и/или резервных копий информации РИС администратор безопасности производит необходимые действия:

– выдача персональных идентификаторов или ключевых носителей средств криптографической защиты информации (СКЗИ) пользователям РИС;

– ведение журналов регистрации, учёта и выдачи носителей информации поэкземплярного учёта СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

– шифрование резервных копий, содержащих ЗИ, обрабатываемую в информационной системе, сертифицированными алгоритмами.

Дополнительные требования к администратору безопасности в связи с использованием средств шифрования данных могут быть определены в специальных регламентах работы с шифрованием информации РИС.

9. Действия по фактам несоблюдения требований по защите информации

При выявлении фактов несоблюдения условий и нарушения требований по защите ЗИ и использования средств защиты, администратор безопасности обязан произвести следующие действия:

- незамедлительно сообщить о происшедшем руководству;
- собрать возможные факты (свидетельства) несоблюдения условий и требований по защите ЗИ и использования средств защиты информации;
- сформировать экспертную комиссию по расследованию инцидента (при необходимости с привлечением внешних экспертов, представителей лицензиатов ФСТЭК России);
- экспертная комиссия составляет заключение условий и требований по защите ЗИ и использования средств защиты информации.

Составленное экспертной комиссией заключение является основанием для наложения административного и (или) дисциплинарного взыскания на виновных лиц.

Экспертная комиссия при расследовании инцидентов, связанных с нарушением обеспечения защищенности ЗИ, вправе производить обследование объектов РИС с согласия лица, ответственного за организацию обработки ЗИ.

10. Порядок приостановки предоставления ЗИ

Администратор безопасности, при получении информации или самостоятельно выявив нарушения порядка предоставления ЗИ, предпринимает следующие действия:

- незамедлительно приостанавливает работу с ЗИ;
- сообщает о происшедшем руководству;
- самостоятельно или с привлечением дополнительных специалистов выявляет причины возникновения нарушения;
- в случае выявления и устранения причины нарушения администратор безопасности восстанавливает работу с ЗИ и сообщает о причинах нарушения и своих действиях руководству;
- в случаях невозможности оперативного выявления причин нарушения, проводится служебное разбирательство. Только по его завершению и устранению причин нарушения восстанавливается работа с ЗИ;
- все действия в процессе реагирования на нарушение порядка предоставления ЗИ должны документироваться администратором безопасности в «Журнале учета нарушений порядка предоставления ЗИ».

11. Права администратора безопасности

Администратор безопасности имеет право:

- требовать от сотрудников соблюдения правил работы со средствами защиты информации, средств криптографической защиты информации, входящими в состав РИС;
- осуществлять взаимодействие (давать необходимые рекомендации, проводить консультации, получать требующиеся сведения) с сотрудниками по вопросам эксплуатации технических и программных СЗИ с целью улучшения качества их работы, а также своевременного предупреждения аварийных ситуаций.

12. Ответственность администратора безопасности

Администратор безопасности несёт ответственность:

– за неисполнение (ненадлежащее исполнение) своих обязанностей, предусмотренных настоящей инструкцией.

– за совершенные в процессе осуществления своей деятельности правонарушения – в пределах, определённых действующим административным, уголовным и гражданским законодательством Российской Федерации.

– за причинение материального ущерба – в пределах, определённых действующим трудовым, уголовным и гражданским законодательством Российской Федерации.

1. Общие положения Инструкция лица, ответственного защиту информации в федеральном государственном бюджетном образовательном учреждении высшего образования «Орловский государственный университет имени И.С. Тургенева» (далее - Инструкция), разработана в соответствии с требованиями существующих законодательно - нормативных документов Российской Федерации, Орловской области и документов федерального государственного бюджетного образовательного учреждения высшего образования «Орловский государственный университет имени И.С. Тургенева» (далее - ОГУ имени И.С. Тургенева) в области безопасности информации. Настоящая Инструкция закрепляет обязанности, права и ответственность лица, ответственного за защиту информации (организацию обработки персональных данных) в ОГУ имени И.С. Тургенева. Лицо, ответственное за организацию обработки персональных данных, в своей работе руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», иными нормативными правовыми актами Российский Федерации, Орловской области, настоящей Инструкцией, а также иными локальными нормативными актами ОГУ имени И.С. Тургенева, регламентирующими вопросы обработки конфиденциальной информации (персональных данных). 2 Обязанности лица, ответственного за защиту информации (организацию обработки персональных данных) 2.1 Лицо, ответственное за защиту информации (организацию обработки персональных данных) в ОГУ имени И.С. Тургенева обязано: - осуществлять внутренний контроль за соблюдением всеми сотрудниками ОГУ имени И.С. Тургенева законодательства Российской Федерации о защите информации (персональных данных), в том числе требований к защите информации (персональных данных); - доводить до сведения сотрудников ОГУ имени И.С. Тургенева положения законодательства Российской Федерации о защите информации (персональных данных), локальных актов по вопросам обработки конфиденциальной информации (персональных данных), требований к защите информации (персональных данных); - организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и осуществлять контроль за приемом и обработкой указанных обращений и запросов. 3. Права лица, ответственного за организацию обработки персональных данных 3 3.1. Лицо, ответственное за защиту информации (персональных данных), имеет право: - принимать решения в пределах совей компетенции; требовать от сотрудников ОГУ имени И.С. Тургенева соблюдения действующего законодательства Российской Федерации по защите информации, а также локальных нормативных актов ОГУ имени И.С. Тургенева по защите информации (персональных данных); - контролировать в ОГУ имени И.С. Тургенева осуществление мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», другими нормативными правовыми актами Российский Федерации, Орловской области по защите информации (персональных данных) и принятыми в соответствии с ними нормативными правовыми актами; - взаимодействовать с руководством и иными структурными подразделениями ОГУ имени И.С. Тургенева по вопросам обработки конфиденциальной информации (персональных данных). 4. Ответственность лица, ответственного за защиту информации (организацию обработки персональных данных) 4.1. За ненадлежащее исполнение или неисполнение настоящей Инструкции, а также за нарушение требований законодательства о защите информации (персональных данных) лицо, ответственное за защиту информации (организацию обработки персональных данных) в ОГУ имени И.С. Тургенева, несет предусмотренную законодательством Российской Федерации ответственность.