«Алтайский государственный технический университет им. И.И. Ползунова»
Факультет информационных технологий
Кафедра информатики, вычислительной техники и информационной безопасности

Разработка мер по защите информации в АИС «Сетевой край. Образование»

Выполнил:
Студент 2 курса ФИТ
Группы ИБ-71
Богер Егор

Цель работы:

Разработать меры по защите информации в АИС «Сетевой край. Образование»

Задание к работе:

1. *Поиск и выбор реального объекта защиты (организация, предприятие) Алт.края*
2. *Описание объекта, его характеристика.*
3. *Определение мер, требований и средств для защиты ОИ.*

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационные системы

- Государственные
  - созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов;
- Муниципальные
  - созданные на основании решения органа местного самоуправления;
- Иные

Оператор информационной системы – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке ации, содержащейся в данных.

«Сетевой Город. Образование» — это комплексная автоматизированная информационная система, объединяющая в единую информационную сеть образовательные организации всех типов и органы управления образованием в пределах муниципального образования.

ГЛАВНОЕ УПРАВЛЕНИЕ ОБРАЗОВАНИЯ И МОЛОДЁЖНОЙ ПОЛИТИКИ АЛТАЙСКОГО КРАЯ

«СЕТЕВОЙ КРАЙ. ОБРАЗОВАНИЕ»

РЕГИОНАЛЬНАЯ ИНФОРМАЦИОННАЯ СИСТЕМА В СФЕРЕ ОБРАЗОВАНИЯ

Уникальный идентификационный номер ИС	**10.0000025**
Документ, на основе которого была создана ИС	Постановление Администрации Алтайского края от 26 ноября 2015 г. N 477 "Об утверждении плана мероприятий ("дорожной карты") по созданию регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам"
Номер документа	477
Дата принятия	26.11. 2015 25.04.2017
Орган исполнительной власти Алтайского края, уполномоченный на создание, развитие, модернизацию ИС:	Министерство образования и науки Алтайского края
Орган исполнительной власти Алтайского края или иное юридическое лицо, уполномоченное на эксплуатацию ИС:	Краевое государственное бюджетное учреждение образования "Алтайский краевой информационно-аналитический центр"

Сетевой Город. Образование

Образовательная организация (ОО)

Пользователи ОО:

- Администрация
- Преподаватели
- Учащиеся
- Родители
- Секретарь
- Специалист по кадрам
- Медработник
- Психолог
- Администратор системы
- Технический персонал

Управление образования

Образовательная организация 1

Образовательная организация 2

Образовательная организация N

Интернет

Сервер управления образования

Интернет

- Классный журнал
- Расписание
- Календарно-тематическое планирование
- Учебные курсы
- База данных
- Отчеты ООУ
- Нормативная документация
- Корпоративная почта
- Отчеты УО

Информационные системы

Федеральные

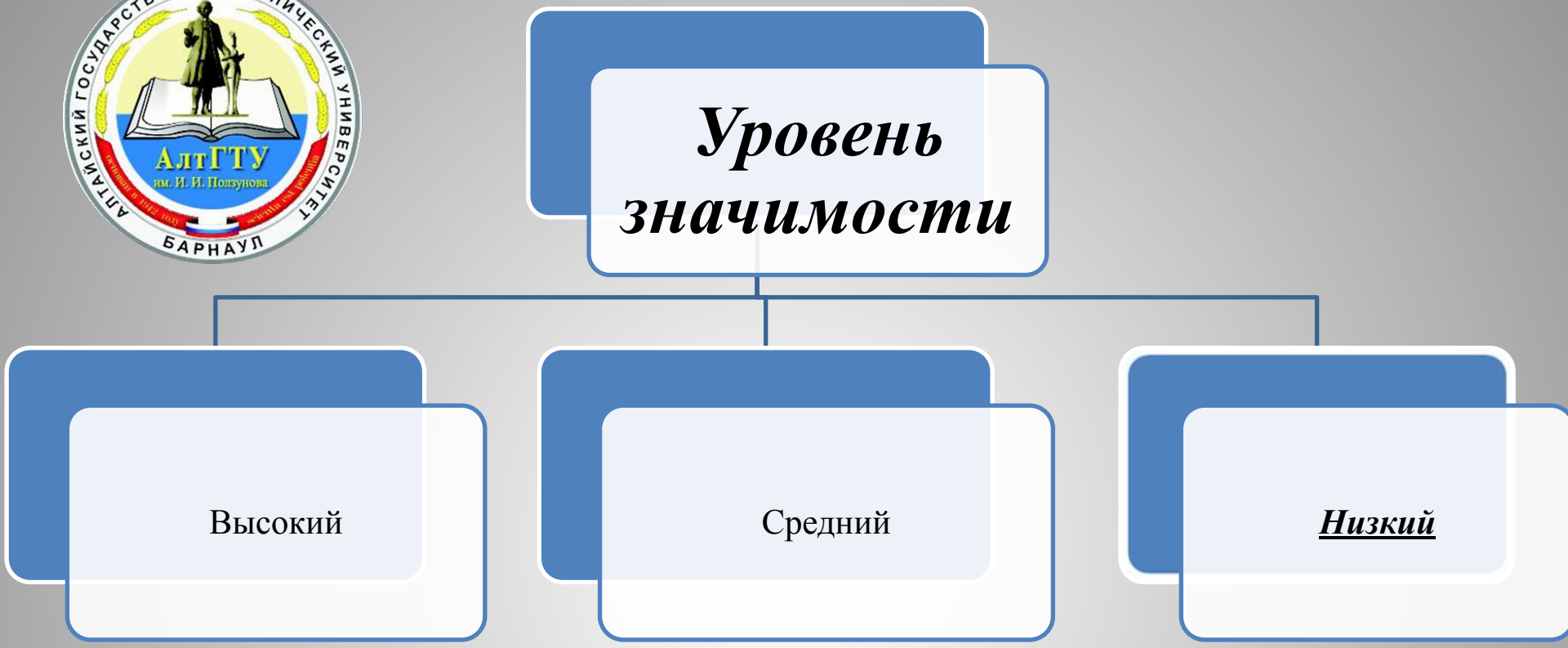
функционирует на территории Российской Федерации (в пределах федерального округа) и имеет сегменты в субъектах Российской Федерации, муниципальных образованиях и (или) организациях.

Региональные

функционирует на территории субъекта Российской Федерации и имеет сегменты в одном или нескольких муниципальных образованиях и (или) подведомственных и иных организациях.

Объектовые

функционирует на объектах одного федерального органа государственной власти, органа государственной власти субъекта Российской Федерации, муниципального образования и (или) организации и не имеет сегментов в территориальных органах, представительствах, филиалах, подведомственных и иных организациях.



АИС «Сетевой край. Образование» имеет Федеральный масштаб и Низкий уровень значимости.

Класс защищенности.

Уровень значимости информации	Масштаб информационной системы		
	Федеральный	Региональный	Объектовый
УЗ 1	К1	К1	К1
УЗ 2	К1	К2	К2
УЗ 3	К2	К3	К3

Исходя из данной таблицы, АИС «Сетевой край. Образование» имеет второй класс защищенности.

Для защиты информации в АИС «Сетевой край. Образование» необходимо пользоваться мерами, прописанными в ***приказе ФСТЭК от 11 февраля 2013 года N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.***

Состав мер защиты информации и их базовые наборы.

Условное обозначение и номер меры	Меры защиты информации в информационных системах
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Защита обратной связи при вводе аутентификационной информации
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)

II. Управление доступом субъектов доступа к объектам доступа (УПД)	
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники

III. Ограничение программной среды (ОПС)	
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов
IV. Защита машинных носителей информации (ЗНИ)	
ЗНИ.1	Учет машинных носителей информации
ЗНИ.2	Управление доступом к машинным носителям информации
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)

V. Регистрация событий безопасности (РСБ)	
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе
РСБ.7	Защита информации о событиях безопасности

VI. Антивирусная защита (АВЗ)	
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
VII. Обнаружение вторжений (СОВ)	
СОВ.1	Обнаружение вторжений
СОВ.2	Обновление базы решающих правил
VIII. Контроль (анализ) защищенности информации (АНЗ)	
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе

IX. Обеспечение целостности информационной системы и информации (ОЦЛ)	
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)
X. Обеспечение доступности информации (ОДТ)	
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование
ОДТ.4	Периодическое резервное копирование информации на резервные машинные носители информации
ОДТ.5	Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала
ОДТ.6	Кластеризация информационной системы и (или) ее сегментов
ОДТ.7	Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации

XI. Защита среды виртуализации (ЗСВ)	
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей

XII. Защита технических средств (ЗТС)	
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр

XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	
ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы
ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи
ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств
ЗИС.7	Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода
ЗИС.8	Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи
ЗИС.9	Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации

ЗИС.11	**Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов**
ЗИС.12	Исключение возможности отрицания пользователем факта отправки информации другому пользователю
ЗИС.13	Исключение возможности отрицания пользователем факта получения информации от другого пользователя
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы
ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе
ЗИС.22	Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы
ЗИС.23	Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями
ЗИС.24	Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения
ЗИС.30	Защита мобильных технических средств, применяемых в информационной системе

Вывод:

В ходе данной работы была проанализирована выбранная ГИС: ей был присвоен класс защищенности, а также был определен состав мер по защите информации, которая хранится в ней.