Августовский педагогический совет

«Безопасность цифровой образовательной среды современной образовательной организации»

2022

к.т.н., зав. кафедрой цифрового образования и информационной безопасности
МИШИН Денис Вячеславович

Цифровая образовательная среда (ЦОС) - открытая совокупность ИС, оборудования, цифрового информационного и образовательного контента, предназначенная для задач управления ОО и реализации ОП (в том числе с применением ЭО и ДОТ), обеспечивающая доступ к образовательным услугам и сервисам в электронном виде и коммуникацию.

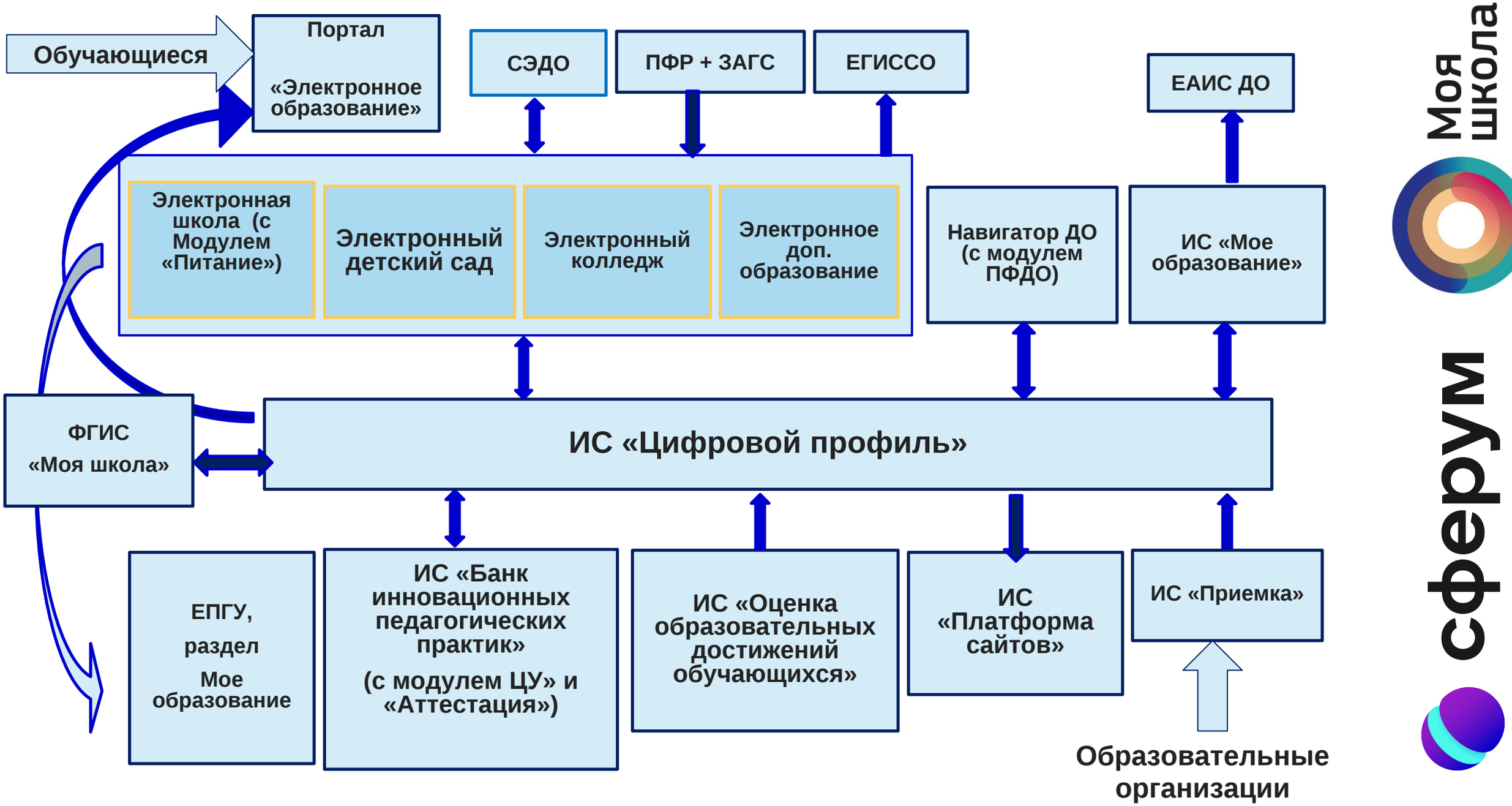
Программная платформа ЦОС

Цифровой информационный и образовательный контент

ИТ инфраструктура

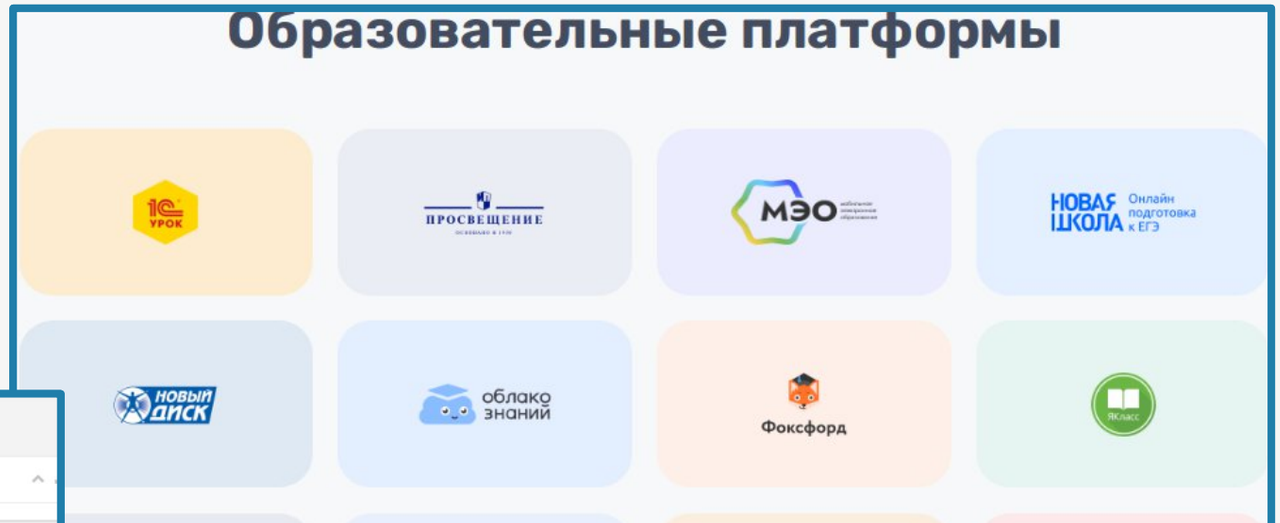
Организация взаимодействия региональных ИС системы образования Владимирской области

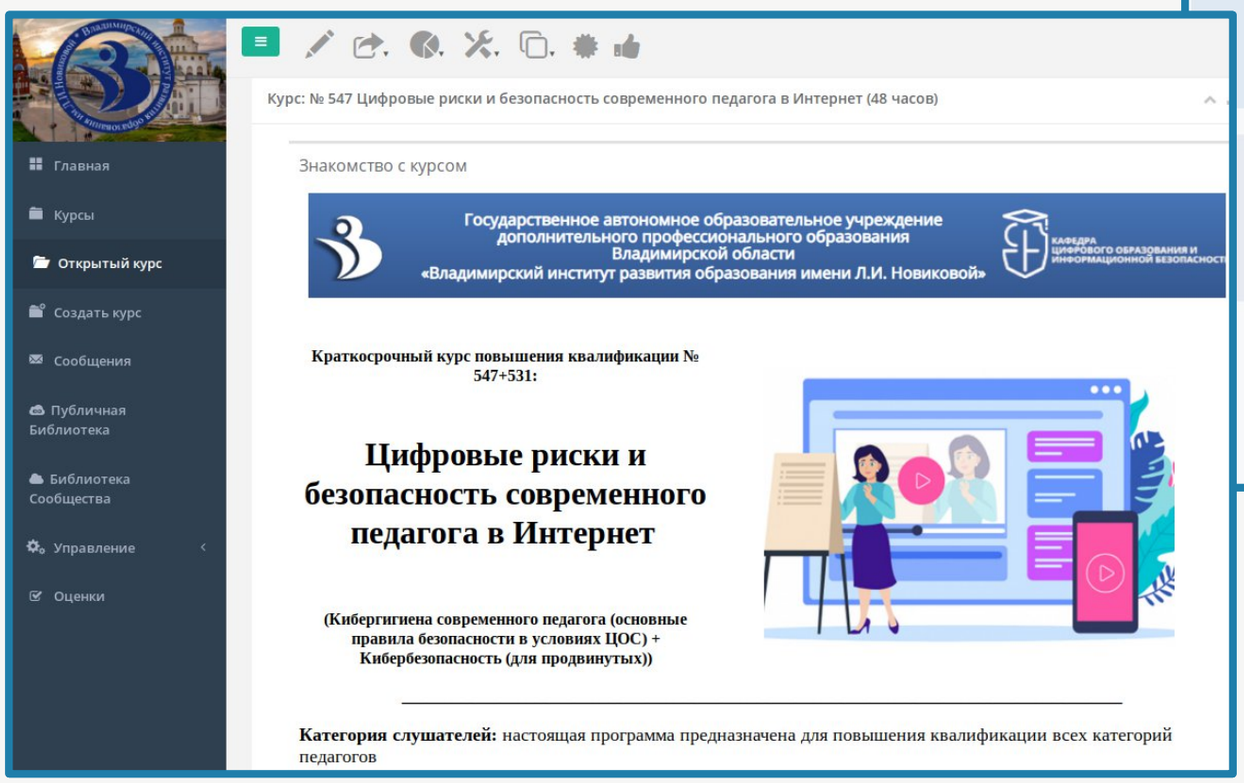
Программная платформа ЦОС – совокупность Федеральных и региональных информационных систем - ГИС РС Контингент (комплекс АИС системы образования Владимирской области), ЕПГУ, ЕСИА, ФГИС Моя школа, ФИС ФРДО, ЕАИС ДО и т.д.), системы видео-конференц связи (Сферум) и соц. сеть образования.

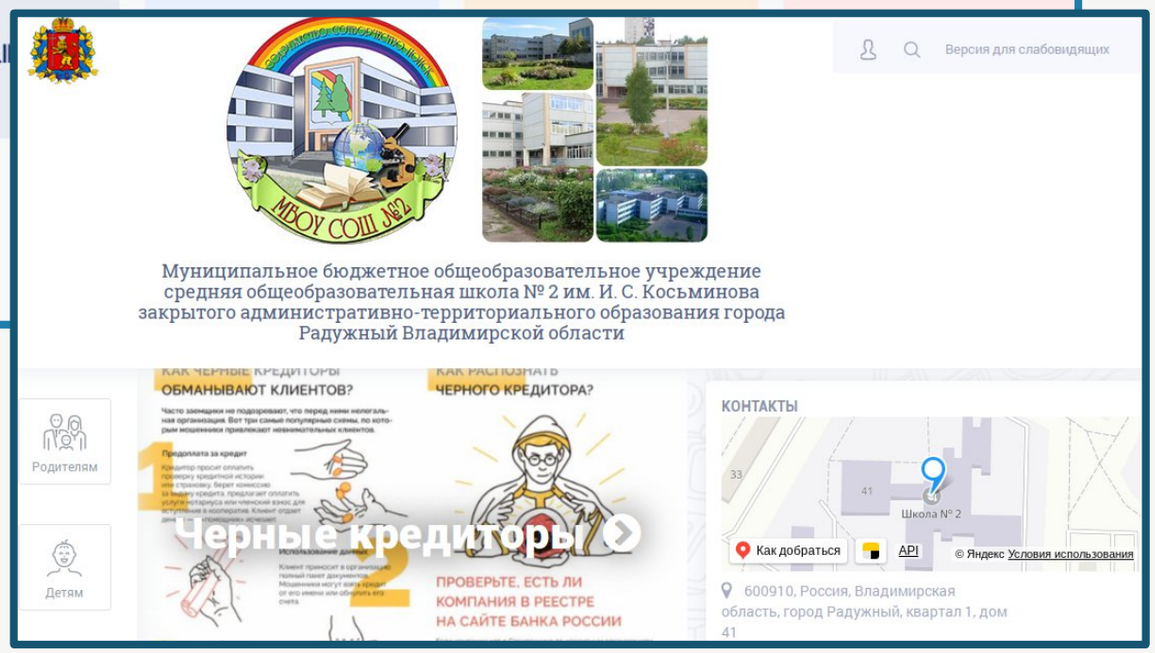


Цифровой информационный и образовательный контент (курсы СЭДО ВО, уроки в системе “Цифровой урок”, электронные учебники, инструменты создания, модерации, воспроизведения контента, виртуальные лаборатории, библиотеки верифицированого образовательного контента, образовательные платформы партнёров и т.д.); официальный сайт ОО, данные АИС (включая ПДн).

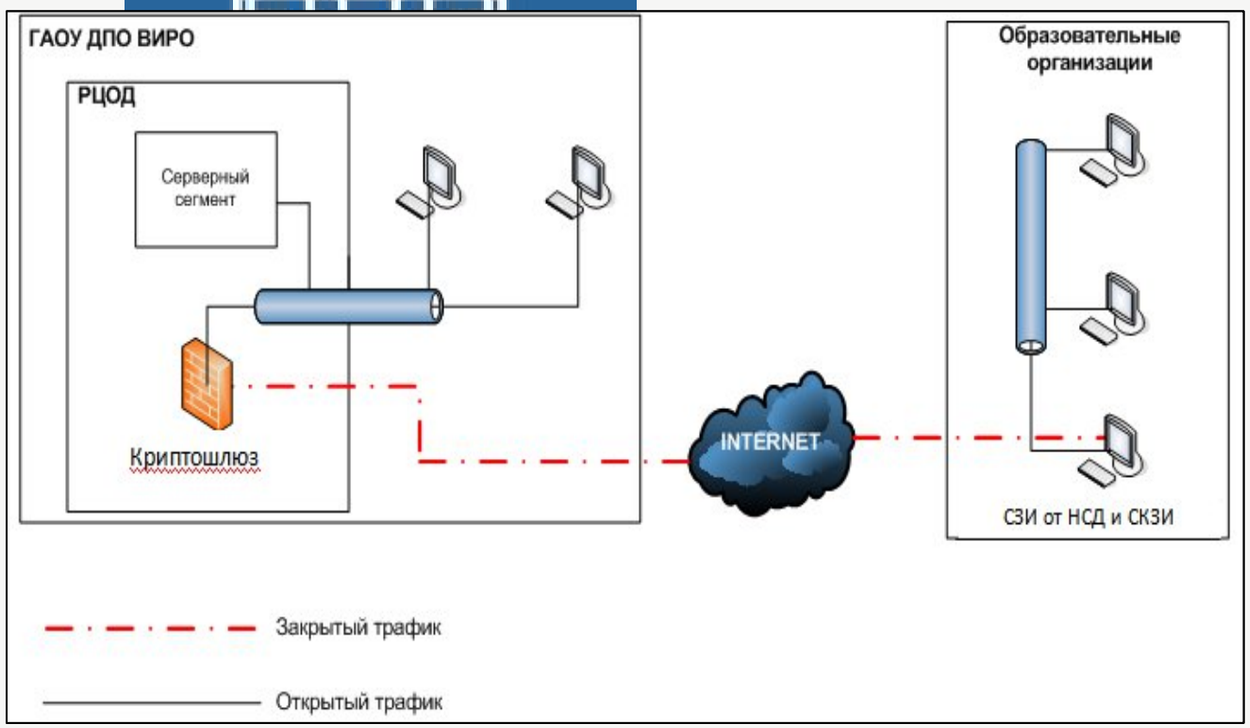
АИС «ЭЛЕКТРОННЫЙ ДЕТСКИЙ САД»
АИС «ЭЛЕКТРОННАЯ ШКОЛА»
АИС «ЭЛЕКТРОННЫЙ КОЛЛЕДЖ»
АИС «ЭЛЕКТРОННОЕ ДОПОЛНИТЕЛЬНОЕ ОБРАЗОВАНИЕ»





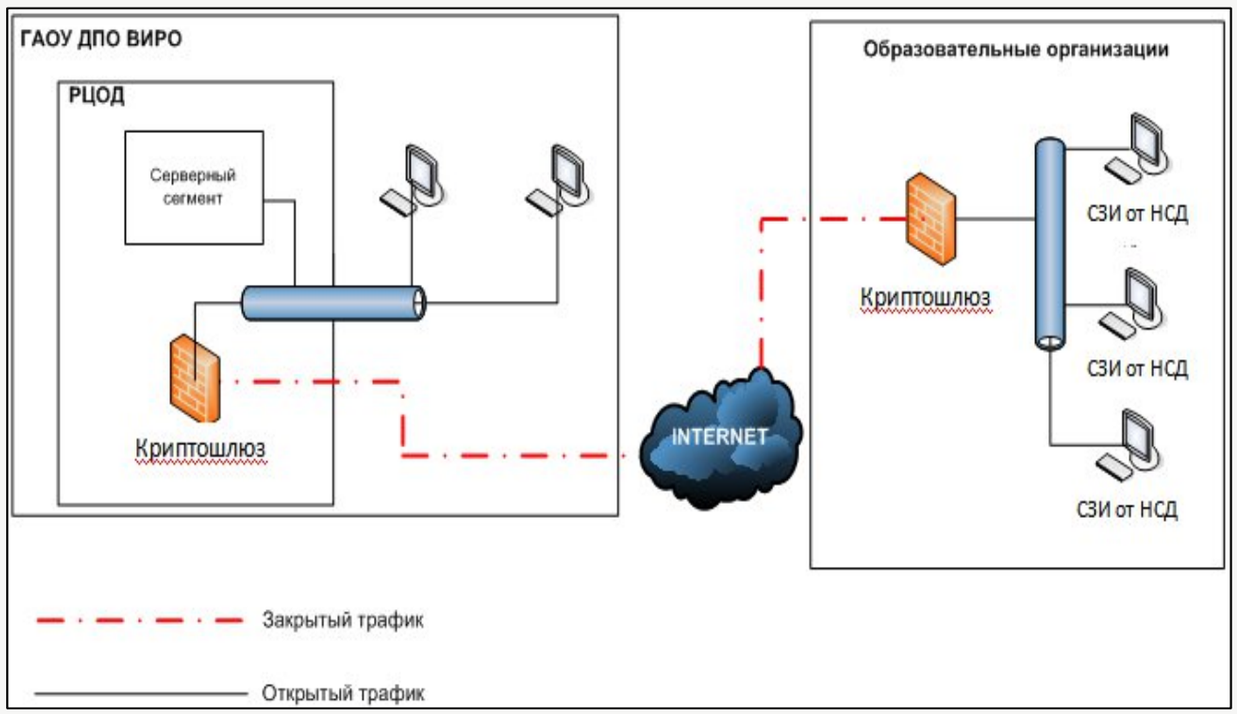


ИТ инфраструктура – высокоскоростной интернет, современная материально-технической база ОО (камеры, ноутбуки, интерактивные доски, АРМ педагога и т.д.); надёжное и функциональное системное и прикладное ПО;
РЦОД и информационно-телекоммуникационная инфраструктура, включая защищенные каналы связи (ЗСПД, ЕСПД)



Защита информации в ЗСПД СОВО осуществляется в соответствии с НПА РФ в области защиты ПДн и иной конфиденциальной информации, требованиями по использованию СКЗИ

Безопасность информации в ЗСПД СОВО обеспечивается комплексом организационных, технических мер в соответствии с требованиями регуляторов в области информационной безопасности (ФСТЭК и ФСБ РФ).



Организация взаимодействия региональных ИС системы образования Владимирской области

ЗИ на региональном и Федеральном уровне

Инструменты МинПросвещения

Библиотеки контента, образовательные платформы партнёров и т.д.

ФИС ФРДО и др. ФГИС

Региональные АИС и АИС ОО, хранимые в РЦОД

ЕСПД?

ЕСПД?

Интернет

Защита каналов

ЗСПД СОВО ЕСПД

ЗСПД СОВО ЕСПД

ЗИ на уровне ОО

Образовательная организация. Локальные ИС, ЛВС

ЦОС образовательной организации

ЗИ на уровне ОО

Безопасность инфраструктуры ЦОС образовательной организации
– требования регуляторов по ЗИ для ИСПДн (ГИС);
– защита каналов связи (ЗСПД СОВО, ЕСПД и т.д.);
– обеспечение работоспособности и производительности цифрового оборудования и ЛВС.

Безопасность ИС образовательной организации – региональные АИС (ЭШ, ЭДО, ...), СЭДО ОО, Сферум и т.д.

Безопасность при использовании ИС партнёров, ЦОР.

Терминология

В контексте ЦОС

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ – состояние защищенности информационных ресурсов ЦОС и поддерживающей инфраструктуры (на Федеральном, региональном, муниципальном и уровне ОО) от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам образовательного процесса, использующим ЦОС

конфиденциальность	*целостность*	*доступность*
состояние **информации**, при котором доступ к ней осуществляют только субъекты, имеющие на него право	состояние **информации**, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право	состояние **информации**, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.

Терминология

ЗАЩИТА ИНФОРМАЦИИ в ЦОС - деятельность, направленная на обеспечение информационной безопасности (конфиденциальности, целостности и доступности) информационных ресурсов ЦОС и поддерживающей инфраструктуры

Важно понимать, что универсальных методов ЗИ не существует, поэтому часто рассматривают некую совокупность неформальных рекомендаций по построению систем ЗИ и принятия определенных мер, направленных на:

1) обеспечение защиты информации **от неправомерного доступа**, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение **конфиденциальности информации** ограниченного доступа (например, персональных данных - ПДн);

3) реализацию **права на доступ** к защищаемой информации.

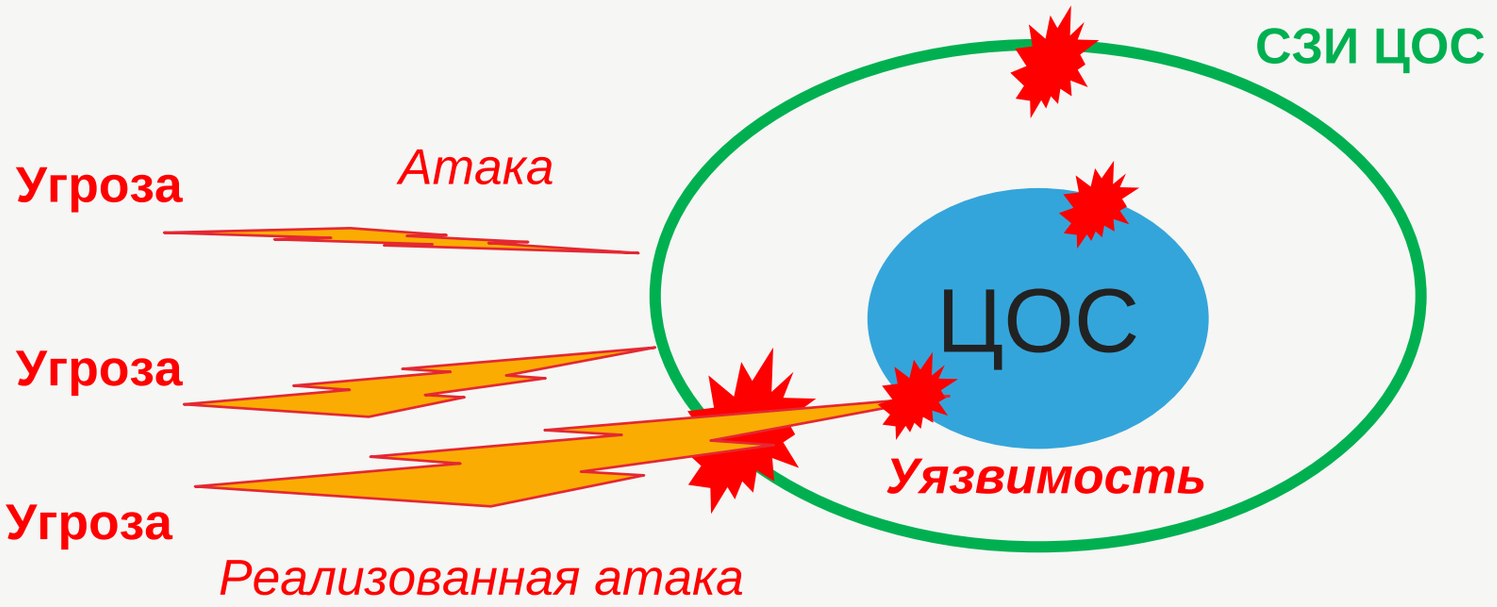
Рассматривая вопросы безопасности ЦОС, можно говорить о наличии некоторых «желательных» состояний системы, через которые и описывается ее «защищенность» или «безопасность». Чтобы указать на причины выхода информационной системы из безопасного состояния, применяются понятия «**угроза ИБ**» и «**уязвимость**».

Угроза ИБ ЦОС - это потенциальная опасность для информации или информационной инфраструктуры ЦОС.

Угрозой ИБ ЦОС является, если кто-то или что-то выявит наличие определенной уязвимости ЦОС и использует ее против образовательной организации или участников образовательного процесса (руководителя, педагога, ученика, родителя).

Уязвимость ЦОС - это недостаток в программном обеспечении, оборудовании или процедуре, который может быть использован для реализации **угрозы ИБ ЦОС**.

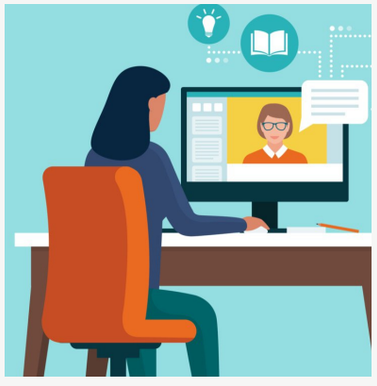
Уязвимость ЦОС - это отсутствие, ошибочная конфигурация или неправильное использование защитных мер ЦОС.



Контрмеры (или защитные меры) - это меры, внедрение которых позволяет снизить уровень риска для ЦОС.

Наиболее характерные угрозы ЦОС уровня ОО сегодня:

1. нарушение конфиденциальности ПДн (или другой информации ограниченного доступа), автоматизировано обрабатываемой в образовательной организации
2. нарушение требований законодательства в области ИБ и ЗИ;
3. нарушение целостности и доступности данных об участниках образовательного процесса, результатах образовательной деятельности, данных об ОО, данных на официальном сайте образовательной организации;
4. нарушение целостности цифрового информационного и образовательного контента;
5. нарушение доступности цифрового информационного и образовательного контента.



Наиболее характерные уязвимости ЦОС на уровне ОО сегодня:

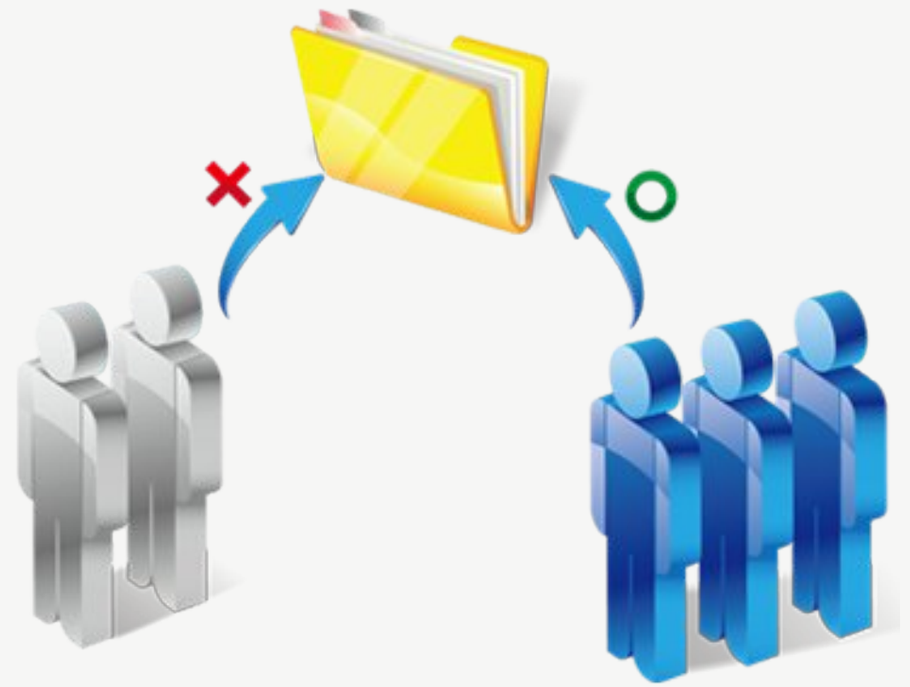
- отсутствие актуальной / невыполнение парольной политики и политики управления пользователями;
- отсутствие актуальной / невыполнение политики работы с электронной почтой;
- отсутствие актуальной / невыполнение политики работы с ресурсами ЦОС в интернет;
- отсутствие актуальной / невыполнение антивирусной политики;
- отсутствие актуальной / невыполнение политики обработки персональных данных;
- отсутствие актуальной / невыполнение политики резервного копирования;
- использование в ЦОС “недоверенного” системного и прикладного ПО (НДВ);
- недостаточно высокий уровень компетенций в области работы с отечественным ПО;
- недостаточно высокий уровень компетенций в области цифровой безопасности.

Управление пользователями в ЦОС. Парольная политика образовательной организации. Защита ЦОС от НСД

к.т.н., зав. кафедрой цифрового образования и информационной безопасности
МИШИН Денис Вячеславович

Управление доступом – это механизм безопасности, который управляет процессом взаимодействия пользователей с ЦОС и ресурсами, а также информационных систем между собой

Управление доступом крайне важно, т.к. **является первой линией обороны** в борьбе с несанкционированным доступом к АИС и разделяемым сетевым ресурсам.



Управление доступом защищает информационные системы (ИС) и их ресурсы от несанкционированного доступа (**НСД**) и принимает участие в определении уровня авторизации **после успешного прохождения процедуры аутентификации**.

Управление доступом позволяет управлять, ограничивать, контролировать и защищать (т.е. обеспечивать) доступность, целостность и конфиденциальность ресурсов защищаемой ИС.

Любому пользователю (процессу) информационной системы, чтобы получить доступ к ресурсам АИС ОО, необходимо выполнить три шага.

Только при успешном выполнении всех этих шагов пользователю должен предоставляться доступ к ресурсам.

Кроме того, необходимо отслеживать действия пользователей, используя для этого средства ведения учета (протоколирование и аудит).

1. представиться системе (назвать себя - ***идентифицироваться***);
2. подтвердить, что он тот, за кого себя выдает (***аутентифицироваться***)
3. подтвердить, что имеет необходимые права и привилегии для выполнения действий, которые он запросил (***авторизоваться***)

АДМИНИСТРИРОВАНИЕ управлением доступа к ресурсам ЦОС образовательной организации — процесс управления доступом субъектов ЦОС (пользователей) ОО к ресурсам ЦОС ОО.

Задачи **администрирования** включают:

1. Создание/удаление идентификатора субъекта (учетной записи пользователя) в системе (или проверка и подтверждение при самостоятельной регистрации);
2. Управление данными пользователя, используемыми для его аутентификации (создание и смена пароля и т. п.);
3. Управление правами доступа пользователя к ресурсам (объектам) системы.

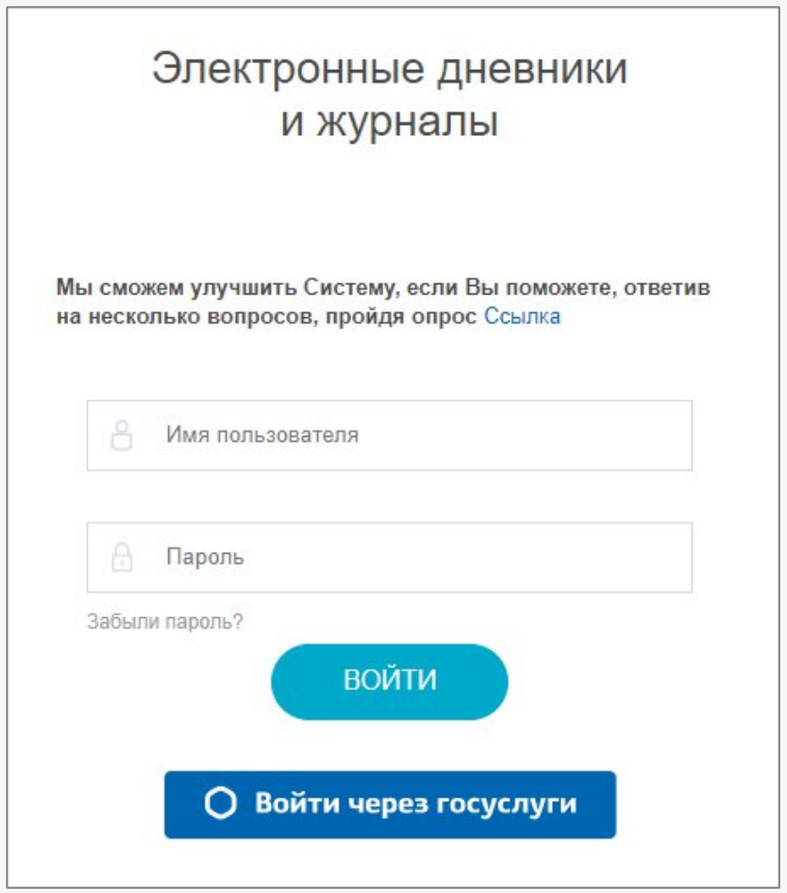
Задачи **администрирования** включают:

1 - Создание/удаление идентификатора субъекта (учетной записи пользователя) в системе (или проверка и подтверждение при самостоятельной регистрации);

- Какими документами ОО регламентируется управление пользователями?
- Если ли в ОО регламент управления пользователями / администраторами?
- Есть перечень администраторов АИС? Актуален ли он?
- Кто создаёт/блокирует/удаляет пользователей в АИС? На каком основании? В какие сроки?
- Кто создаёт/изменяет пароль?
- Обязателен ли вход через ЕСИА?
- Проводится ли контроль соблюдения политики?

Задачи **администрирования** включают:

2 - Управление данными пользователя, используемыми для его аутентификации (создание и смена пароля и т. п.);



- Если ли в ОО парольная политика? Другие документы (формы заявок, листы ознакомления и т.д.)?
- Пользователи / администраторы ознакомлены с данными документами?
- Журнал/листы ознакомления ведутся?
- Актуальны ли требования парольной политики ОО современным реалиям?
- Отличаются ли требования для обычных и привилегированных пользователей?
- Может ли пользователь сам изменять пароль?
- Как реагировать при компрометации пароля?
- Проводится ли контроль соблюдения политики?

Наиболее распространенные ошибки использования паролей:

Критические ошибки

Критические ошибки - Приводят к фатальным последствиям. Являются результатом равнодушного отношения ОО к ИБ.

1. Примитивные пароли или пароли по умолчанию
2. Одинаковые пароли для всех программ и сервисов
3. Открыто записанные логины и пароли
4. Легко восстанавливаемые пароли (сохранённые)
5. Скомпрометированные и просроченные пароли

Наиболее распространенные ошибки использования паролей: **Серьезные ошибки**

Серьезные ошибки - Ведут к серьезным негативным последствиям. Являются результатом недостаточных знаний в области ИБ.

1.Короткие пароли

2.Очень сложные пароли

3.Неграмотное использование спецсимволов

4.Игнорирование альтернативных средств защиты

Недочеты и рекомендации

1.Часто сменяемые пароли

2.Адекватное отношение к периодической смене паролей

Программа «минимум» требований к паролю

1. Пароль должен быть известен только владельцу учетной записи; Запрет передачи пароля по сети;

2. Установление минимальной длины пароля:

- **Для администратора – от 14 символов;**
- Для педагогов – **от 10 символов;**
- Для учеников – **от 8 символов.**

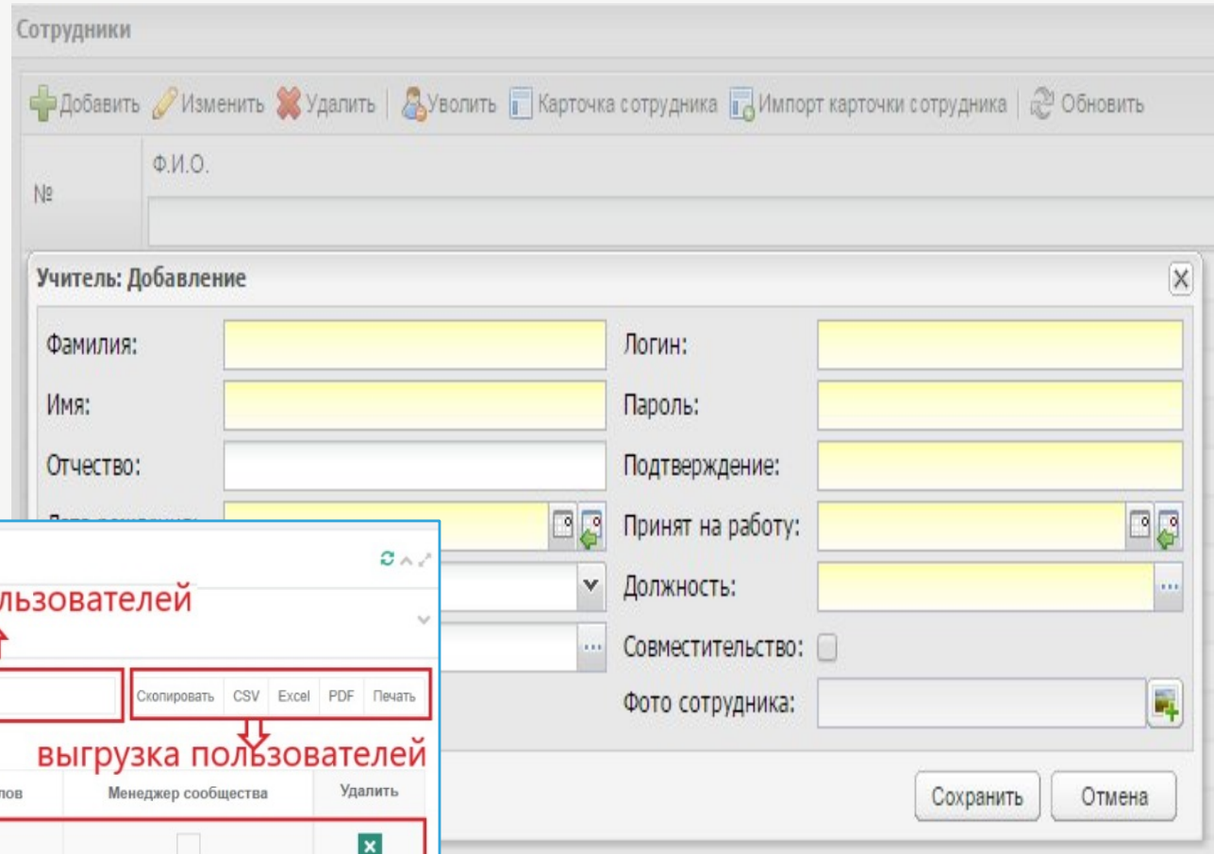
3. Выполнение требований по мощности алфавита паролей (0-9)(` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /) (aA-zZ)

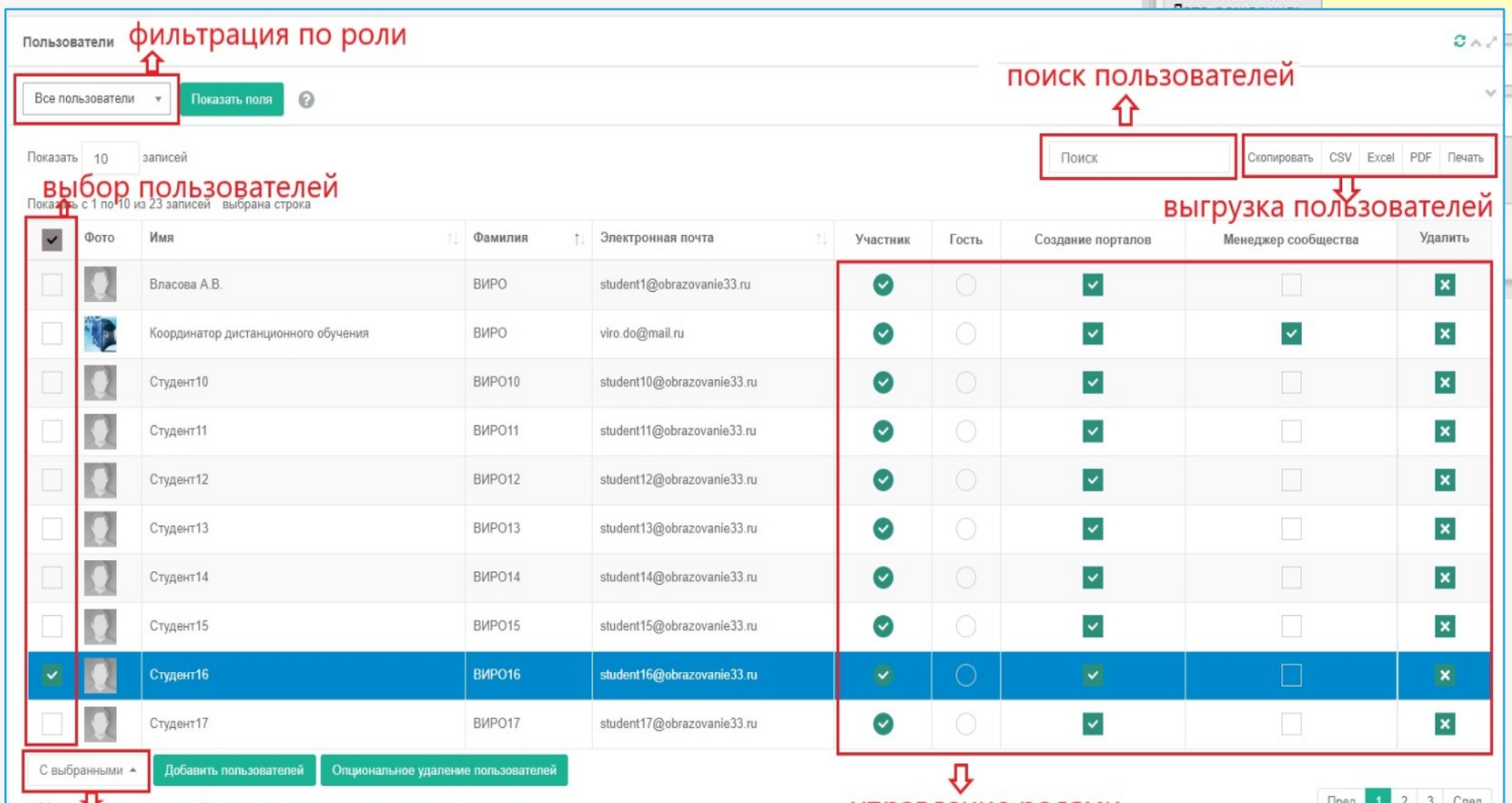
4. Корректная настройка восстановления паролей

Задачи **администрирования** включают:

3 - Управление правами доступа пользователя к ресурсам (объектам) ЦОС.

- Соответствует ли роль пользователя в ИС решаемым задачам и исполняемым обязанностям?
- Сколько администраторов в ОО?





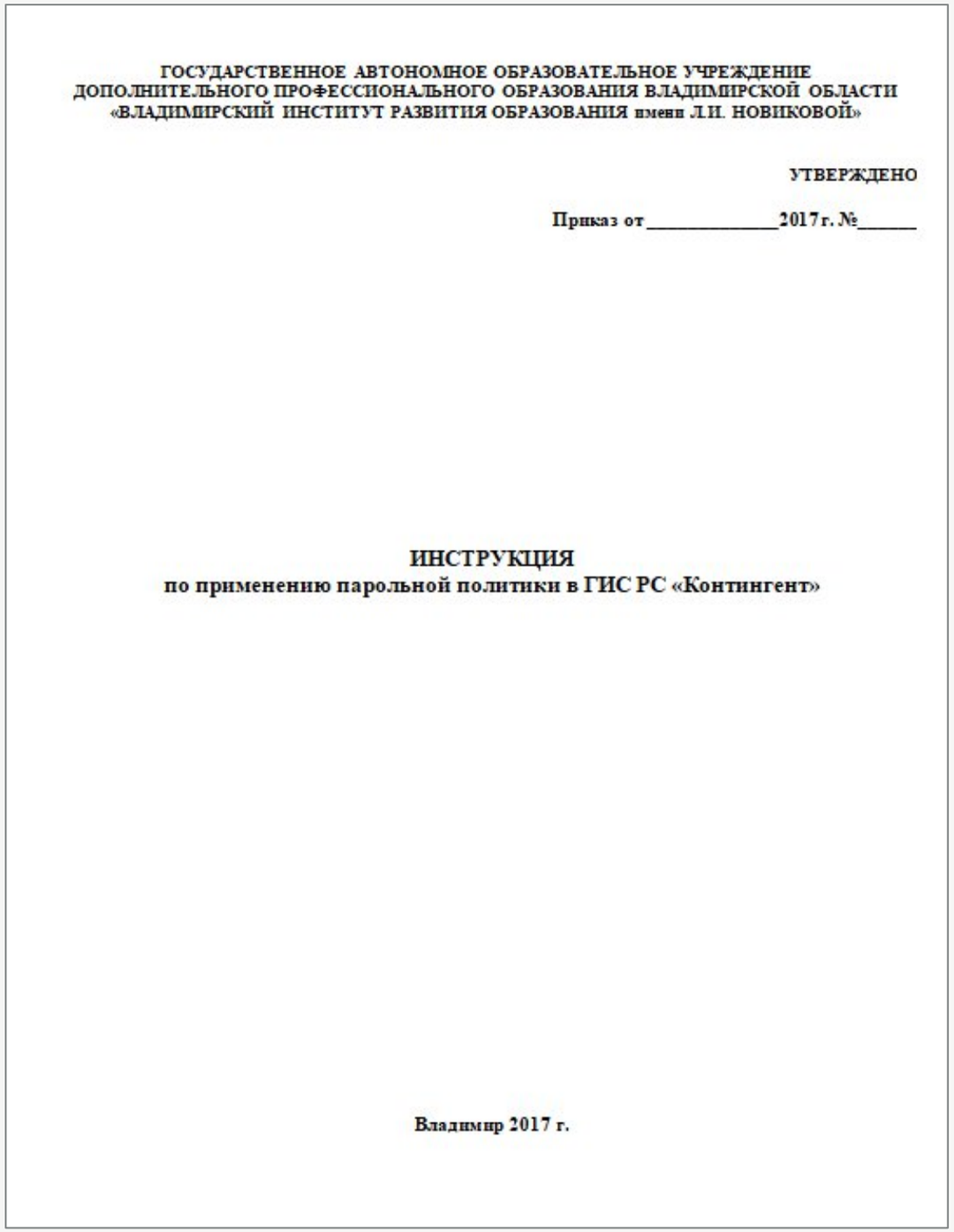
Типовое содержание парольной политики в ЦОС ОО

1. Общие положения (для какой ОО и для какой системы; цель документа);

2. Общие требования к паролям (требования к паролям для АРМ, администраторов / пользователей АИС; ознакомление с политикой; правила смены/обновления пароля; правила хранения паролей);

3. Действия при компрометации пароля (действия пользователя; действия администратора);

4. Проверка соблюдения парольной политики (ответственность за несоблюдение; периодичность проверок; методика проверок; журнал/акт проверок)



ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ ВЛАДИМИРСКОЙ ОБЛАСТИ
«ВЛАДИМИРСКИЙ ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ имени Л.И. НОВИКОВОЙ»

УТВЕРЖДЕНО

Приказ от _____2017 г. №_____

ИНСТРУКЦИЯ
по применению парольной политики в ГИС РС «Контингент»

Владимир 2017 г.

Что сделать в первую очередь?

1. Разработать регламент управления пользователями и парольную политику с учётом используемых в ОО АИС и других особенностей;
2. Утвердить документы у руководства;
3. Провести ознакомление с парольной политикой **всех пользователей ПОД ПОДПИСЬ (указать ответственность);**
4. **Отключить неиспользуемые и тестовые учётные записи;**
5. **Провести проверку паролей на соответствие требованиям, сменить пароли;**
6. В случае необходимости провести обучение по основам ИБ, цифровым рискам и т.д. (на уровне ОО или в ВИРО);
7. Разработать методику и план периодических проверок соблюдения парольной политики;
8. Очистить сохранённые пароли в браузерах компьютеров ОО.
9. Рекомендовать использовать многофакторную аутентификацию и ЕСИА.

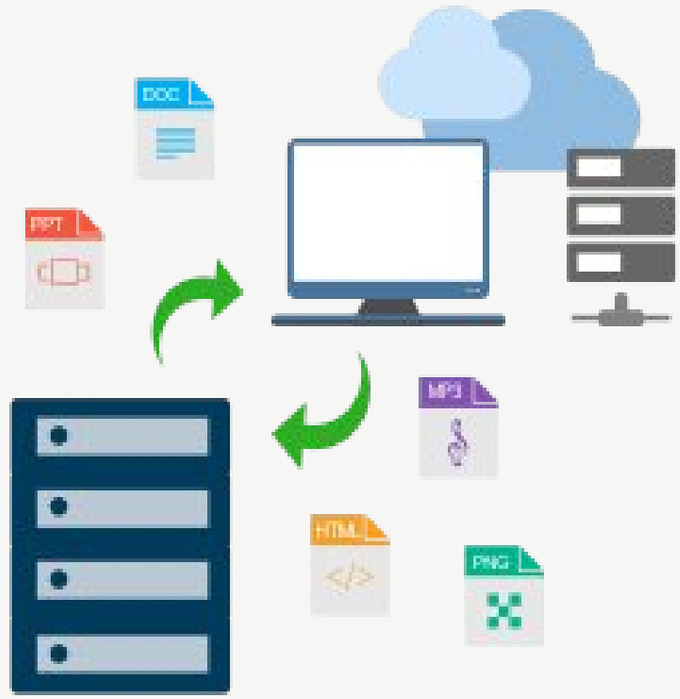
Безопасность цифровых данных в ЦОС образовательной организации. Резервное копирование

Резервное копирование (backup copy) – это создание копии цифровых данных на дополнительном носителе информации (другом компьютере, внешнем жестком диске, CD/DVD-диске, флэшке, в облаке и т.д.).

Резервное копирование в ЦОС необходимо для восстановления данных АИС ОО (и других), если они повреждены в основном месте их хранения.

Почему теряются данные? *Поломка компонентов компьютера или сервера; Программный сбой; Вредоносные программы; Злоумышленники (разного уровня); Пользователь ЦОС.*

Если нет актуальной резервной копии на уровне образовательной организации, то **восстановить важные документы** для отдельной ОО из региональной копии может быть сложно и очень долго!



Чтобы резервное копирование в ЦОС было эффективным, следует учитывать следующие правила:

1) Делайте резервную копию регулярно. В процессе разработки резервную копию курса следует делать после внесения в его содержание каких-либо значительных изменений. Такие копии могут создавать сами разработчики курсов, администратору достаточно обучить разработчиков этой несложной задаче. Администратору же следует делать резервные копии всех обучающих курсов, которые готовятся к внедрению в учебный процесс.

2) У вас должно быть **не менее двух копий данных на разных видах носителей** (например, одна копия на внешнем жестком диске, вторая на DVD-диске, третья на сервере в облаке). Очевидно, что в самый ответственный момент у Вас может не оказаться под рукой диска с резервной копией или диск окажется испорченным. Наличие нескольких резервных копий позволит избежать многих неприятностей и оказать реальную помощь разработчику курса.

3) Копии должны храниться отдельно, одна из копий должна быть в другом компьютере, в другом кабинете или даже здании.

4) После резервного копирования **отключайте внешний накопитель от компьютера** (чтобы избежать воздействия вредоносного ПО на копии и проблем с питающим напряжением).

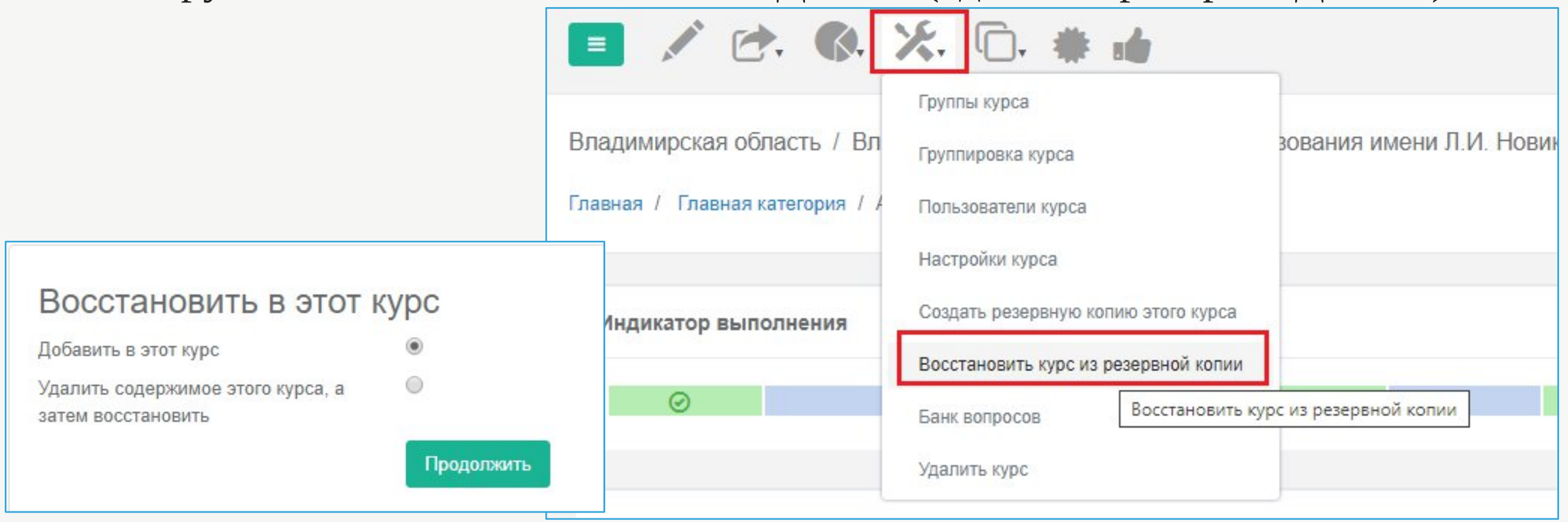
5) Всегда **проверяйте созданные копии на возможность восстановления!** (хуже всего, когда Вы думаете, что резервная копия есть, но она повреждена/не читается/забыли пароль… и это становится известно на стадии восстановления данных).

Что делать?

Организовать (разработать регламент, обучить и т.д.) периодическое резервное копирование наиболее чувствительных данных ЦОС на уровне ОО и каждого отдельного педагога.

На примере **СЭДО:**

- создание резервных копий курсов (педагоги, имеющие право на редактирование курса);
- выгрузка результатов обучения (оценки) и т.д.;
- выгрузка списка пользователей СЭДО ОО (администратор СЭДО ОО).



Безопасность цифровых устройств и других элементов ИТ инфраструктуры ЦОС ОО

Терминология

Для системы защиты информации в ИСПДн и ГИС обязательны для выполнения требования регуляторов в области ИБ РФ (ФСТЭК, ФСБ)

РОСКОМНАДЗОР

Организация обработки и обеспечения безопасности персональных данных

Организация обработки

- Трудовой кодекс Российской Федерации
- 152-ФЗ от 27.07.2006 «О персональных данных»
  - № 211 от 21.03.2012
  - № 1119 от 01.11.2012
  - № 687 от 15.09.2008

Обеспечение безопасности

- 4 НМД ФСТЭК
- 4 НМД ФСБ

Обеспечение безопасности цифровых устройств и других элементов ИТ инфраструктуры ЦОС ОО невероятно важно!

Что сделать?

1. провести инвентаризацию приложений и веб-сервисов, используемых в ОО и доступных из сети Интернет;
2. отключить неиспользуемые службы и веб-сервисы (например старые версии сайта и т.д.);
3. исключить применение подсчета и сбора данных о посетителях, сервисов предоставления информации о местоположении и иных сервисов, разработанных иностранными организациями;
4. убедиться, что сетевое взаимодействие с сайтом происходит по защищенным протоколам (**HTTPS**, SSH и другим);
5. убрать со страниц сайта и курсов в СЭДО встроенные видео- и аудио-файлы, «виджеты» и другие ресурсы, загружаемые со сторонних сайтов, заменив их при необходимости гиперссылкой на такие ресурсы;

Обеспечение безопасности цифровых устройств ОО невероятно важно, потому что хранить или получать доступ к конфиденциальной информации сотрудники будут, используя их.

Защитные меры

- Установка надежного пароля на устройствах ОО (компьютере, ноутбуке) и личных (смартфоне, планшете и любых других устройствах); Блокировка при множественных попытках входа;
- Запрет оставления цифровых устройств ОО (где ведутся АИС или обрабатываются ПДн) незаблокированными (в отсутствии сотрудника ОО);
- Настроить автоблокировку на таких устройствах (задача администратора).

Обеспечение безопасности цифровых устройств ОО невероятно важно, т.к. хранить или получать доступ к защищаемой информации ЦОС сотрудники будут, используя данные устройства.

Защитные меры

- Замените стандартные (от производителя) или слабые пароли для управления маршрутизатором или точкой беспроводного (Wi-Fi) доступа на **надежный** пароль;
- Используйте режим наибольшей защиты (возможный) для подключения всех устройств к беспроводной сети (WPA2/WPA3);
- По возможности не используйте беспроводную сеть для АРМ ИСПДн.

Обеспечение безопасности цифровых устройств ОО невероятно важно, т.к. хранить или получать доступ к защищаемой информации ЦОС сотрудники будут, используя данные устройства.

Защитные меры

- Разработайте антивирусную политику ОО;
- Установите авторитетное (только отечественное) антивирусное программное обеспечение (для ИСПДн – сертифицированное ФСТЭК);
- Настройте режимы работы в соответствии с требованиями вашей ОО (в соответствии с антивирусной политикой);
- Настройте авто-обновление баз вирусных сигнатур и убедитесь в корректности обновления;
- Регулярно сканируйте устройства ОО на наличие вредоносных программ (настройте автоматическое сканирование в не учебное время).

Типовое содержание инструкции по организации антивирусной защиты ЦОС ОО

1. Общие положения (для какой ОО и для какой системы; цель документа и т.д.);

2. Общие требования к АВП (лицензия, сертификат, производитель, основные и дополнительные функции; параметры обновления баз сигнатур, периодичность и режимы сканирования);

3. **Инструкции и Порядок работы** со средствами антивирусной защиты пользователей и администратора;

4. Действия при обнаружении вредоносного ПО (действия пользователя; действия администратора);

5. Проверка соблюдения антивирусной политики (ответственность за несоблюдение; периодичность проверок;)

ИНСТРУКЦИЯ
по организации антивирусной защиты ГИС РС «Контингент»

1. Инструкция устанавливает требования антивирусной безопасности для государственной информационной системы «Региональный сегмент единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам» (далее ГИС РС «Контингент») в сегменте, расположенном в государственном автономном образовательном учреждении дополнительного профессионального образования Владимирской области «Владимирский институт развития образования имени Л.И. Новиковой».
2. Общие требования
3. Антивирусные средства защиты должны быть лицензионными и иметь сертификат соответствия требованиям безопасности, выданный Федеральной службой по техническому и экспортной контролю (ФСТЭК) России.
4. Закупка средств антивирусной защиты должна быть централизованной. Все элементы ГИС рекомендуется оснащать одним антивирусным программным продуктом.
5. Параметры антивирусной политики задаются ответственным за организацию обработки ПДн (администратором информационной безопасности).
6. Реализация параметров антивирусной политики осуществляется системным администратором.
7. Антивирусные средства защиты должны функционировать исправно и непрерывно. При сбоях в работе требуется немедленное вмешательство системного администратора для устранения неполадок.
8. При выборе антивирусных средств необходимо так же учитывать его быстродействие, для того чтобы не перегружать системные процессы автоматизированного рабочего места (АРМ) и не создавать затруднений для работы пользователей ГИС.
9. Параметры антивирусной политики
10. Основными параметрами антивирусной политики являются периодичность обновления антивирусных баз, периодичность проверки наличия/отсутствия вирусных заражений и параметры проверки «на лету» при работе в сети Интернет.
11. Обновление антивирусных баз должно осуществлять по мере выхода новых баз. Для этого необходимо настроить каждое АРМ ГИС на обновление из сети Интернет.
12. Периодичность проверки наличия/отсутствия вирусных заражений настраивается в консоли управления антивирусным средством и применяется на каждом АРМ ГИС. Данный параметр устанавливается на один раз в неделю (в любой день) на обеденный перерыв. Проверке должны подвергаться все разделы жесткого диска АРМ. На АРМ ГИС такие настройки делаются непосредственно на месте системным администратором.
13. Параметры проверки «на лету» при работе в сети Интернет должны включать в себя все возможные объекты реагирования. На АРМ ГИС такие настройки делаются непосредственно на месте системным администратором.

Проведение атак на ЦОС может осуществляться через внедрение в обновления иностранного ПО вредоносного программного обеспечения. При этом распространение обновлений с вредоносами может осуществляться через центры обновлений (официальные сайты) разработчиков иностранного ПО, размещаемые в сети «Интернет».

Защитные меры

1. Необходимо (при наличии возможности) **приостановить работы по обновлению применяемого в информационных системах иностранного программного обеспечения и программно-аппаратных средств**, страной происхождения которых является США и страны Европейского союза, а также **исключить их автоматическое централизованное обновление посредством сети «Интернет»**.
2. Необходимо (при наличии возможности) **осуществить переход на преимущественное использование отечественного программного обеспечения**

Нормативная база по переходу на преимущественное использование отечественного программного обеспечения

- Постановление Правительства РФ от 16 ноября 2015 г. No1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд»;
- Федеральный закон от 29.06.2015 № 188-ФЗ “О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и статью 14 Федерального закона «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»
- Необходимость проведения цифровой трансформации именно на базе отечественных решений прямо закреплена в национальной программе (нацпроекте) “Цифровая экономика”;
- Приказ Минкомсвязи России от 20.09.2018 № 486 «Об утверждении методических рекомендаций по переходу государственных компаний на преимущественное использование отечественного программного обеспечения, в том числе отечественного офисного программного обеспечения»
- Письмо Министерства цифрового развития, связи и массовых коммуникаций РФ от 01.04.2022 МШ-П8-1-070-14732 «Об импортозамещении цифровых решений в органах управления РФ»;
- Письмо Департамента образования Владимирской области от 17.08.2021 № ДО-7697-09-08 «О предоставлении дистрибутивов отечественного программного обеспечения»

Популярные отечественные ОС, подходящие для системы образования

В настоящее время на рынке отечественных операционных систем существует большое количество предложений, некоторые из них могут применяться в образовательных организациях Владимирской области.

https://reestr.digital.gov.ru/

Российский | Евразийский

РЕЕСТР ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

ASTRA LINUX®

РЕД ОПЕРАЦИОННАЯ СИСТЕМА

ROSA

alt linux

Безопасность инфраструктуры ЦОС

Основные этапы внедрения отечественного ПО в образовательных организациях Владимирской области

Этап 1 (уровень образовательной организации). Обоснованный выбор операционных систем российского производства для образовательного процесса, инфраструктуры образовательной организации, защищенных АРМ (доступ к ГИС системы образования) на основании следующих критериев:

- наличие ОС в Едином реестре российских программ Минкомсвязи России (https://reestr.minsvyaz.ru/reestr/ https://reestr.digital.gov.ru/),
- совместимость ОС с цифровым оборудованием образовательной организации и средствами защиты,
- популярность ОС на отечественном рынке,
- сроки поддержки ОС,
- стоимость лицензии и технической поддержки,
- наличие курсов повышения квалификации по данной ОС в регионе.

Выбор ОС на данном этапе может быть осуществлён на основе анализа документации и описания решений на официальных сайтах разработчиков отечественного программного обеспечения, а также тестовой установки программного обеспечения в среде виртуализации, например, в VirtualBox.

Основные этапы внедрения отечественного ПО в образовательных организациях Владимирской области

Этап 2. Повышение квалификации администраторов образовательной организации и лиц, ответственных за внедрение операционных систем и офисного ПО российского производства, на тематических курсах по администрированию ОС на базе Linux. Организация взаимодействия с технической и методической поддержкой сотрудников ОО (администраторов) на уровне муниципалитета.

Владимирским институтом развития образования на 2023 год запланированы следующие краткосрочные курсы для администраторов образовательной организации и лиц, ответственных за внедрение операционных систем и офисного ПО российского производства:

- **«Внедрение и администрирование отечественных операционных систем в современной школе и СПО» -** 48 часов (дистанционно);

- **«Основы администрирования отечественных дистрибутивов на базе Linux» -** 18 часов (очно).

Программы данных курсов ориентированы на работу с наиболее популярными отечественными операционными системами, в том числе операционными системами РЕД ОС, Astra Linux, ALT Linux, POCA Linux.

Основные этапы внедрения отечественного ПО в образовательных организациях Владимирской области

Этап 3. Опытная эксплуатация выбранных программных решений.

На данном этапе рекомендуется установить новые операционные системы совместно с имеющимися на компьютерах ОС семейства Windows в режиме двойной загрузки. Также рекомендуется провести тестирование оборудования и ознакомить пользователей (сотрудников образовательной организации и учащихся) с новыми программными решениями.

Основные этапы внедрения отечественного ПО в образовательных организациях Владимирской области

Этап 4. Повышение квалификации сотрудников ОО на тематических курсах по использованию отечественных ОС на базе Linux и офисного ПО. Организация технической и методической поддержки сотрудников на уровне образовательной организации.

Владимирским институтом развития образования на 2023 год запланированы следующие краткосрочные курсы для администраторов образовательной организации и лиц, ответственных за внедрение операционных систем и офисного ПО российского производства:

- **«Использование отечественных операционных систем в учебном процессе образовательной организации»** - 48 часов (дистанционно);
- **«Применение отечественного программного обеспечения в учебном процессе образовательной организации»** - 18 часов (очно);
- **«Основы цифровой грамотности педагогических работников (курс для начинающих)»** - 36 часов (очно-дистанционно);
- **«Информационные и коммуникационные технологии в дошкольном образовании»** - 36 часов (очно);
- **«Использование информационных технологий в профессиональной деятельности педагога (курс для начинающих)»** - 36 часов (очно).

Обновлённые программы данных курсов ориентированы на работу педагога с наиболее популярными отечественными ОС, в том числе операционными системами РЕД ОС, Astra Linux, ALT Linux, POCA Linux, отечественными браузерами и офисными пакетами Мой офис, Libre Office, R7-офис.

Основные этапы внедрения отечественного ПО в образовательных организациях Владимирской области

Этап 5. Работа с родителями. Необходимо разъяснить родителям причины перехода на новое программное обеспечение в образовательной организации, информировать о рисках несовместимости форматов файлов (например, результатов домашней работы) при использовании различных пакетов ПО в образовательной организации и дома, дать рекомендации по установке использованию отечественных ОС, браузеров и офисных программ на домашних компьютерах учащихся.

Большая часть отечественных ОС и офисных пакетов являются бесплатными для домашнего использования.

Этапы 1,2 и этапы 3,4 при благоприятных условиях и в случае готовности образовательной организации могут проводиться одновременно.