3.5 **F** **F a** **К о с о**	**Архитектура IT** Общие требования к ИТ-Инфраструктуре	ИТ инфраструктура должна представлять собой совокупность программных и аппаратных средств, реализующие функции поддержки образовательных процессов, автоматизации функционирования инженерной инфраструктуры здания, функционал защиты информации. Территориально ИТ инфраструктура должна быть расположена в здании проектируемого объекта и на площадках доверенного ЦОД. Ландшафт ИТ инфраструктуры должен включать два логически разделенных контура: • закрытый контур – должен быть предназначен для обработки конфиденциальной информации; • открытый контур – должен быть предназначен для обработки информации общего доступа и информации ограниченного доступа (не включающие конфиденциальную информацию). Взаимодействие между контурами должно осуществляться только через межсетевые экраны, либо однонаправленные шлюзы. Уточнение требований необходимо провести в рамках ЧТЗ.
	Требования к структурным подсистемам и модулям	ИТ-инфраструктура должна включать следующие структурные подсистемы: • Подсистема предоставления данных; • Подсистема передачи данных; • Подсистема обработки данных; • Подсистема хранения данных; • Подсистема инженерной инфраструктуры для ИТ; • Подсистема защиты информации. Подсистема предоставления данных должна включать следующие модули для обеспечения взаимодействия пользователей с ресурсами ИТ-инфраструктуры: • Автоматизированные рабочие места: стационарных пользователей, удаленных пользователей, мобильные пользовательские устройства, специализированные рабочие станции для арены киберспорта; • Средства визуализации, звуковоспроизведения актового зала; • Средства звукозаписи (звукоподготовка медиакомплекса); • Телевизионное оборудование; • Периферийное оборудование; • Интерактивная видеоконференцсвязь с эффектом присутствия; • Телефония; • Интерактивные информационные терминалы. Подсистема передачи данных должна включать следующие модули для обеспечения сетевого взаимодействия между компонентами ИТ-инфраструктуры: • Структурированная кабельная система;

- Магистральные каналы доступа в интернет;
- Сетевое оборудование сети передачи данных;
- Сетевое оборудование беспроводной сети;
- Сети телефонной связи;
- Оборудование передачи видеосигнала;
- Системы удаленного доступа;
- Сети радиовещания;
- Часофикация;
- Система позиционирования.

Для обеспечения сетевого взаимодействия между компонентами ИТ-инфраструктуры необходимо учитывать следующие требования для подключения:

- Коммутаторы уровня доступа должны обеспечивать подключения до 1 Гбит/сек
- Коммутаторы уровня распределения/серверной должны обеспечивать подключения до 10 Гбит/сек
- Коммутаторы уровня ядра сети должны обеспечивать подключения до 40 Гбит/сек
- Скорость подключения к магистральным каналам связи должна быть не менее 2 Гбит/сек до каждого оператора связи (операторов должно быть не менее двух) с возможностью расширения канала связи.

Подсистема обработки данных должна включать следующие модули:

- Вычислительные ресурсы закрытого контура;
- Вычислительные ресурсы открытого контура;
- Вычислительные ресурсы средств технической защиты;
- Вычислительные ресурсы инженерных систем здания

Вычислительные ресурсы должны включать аппаратные компоненты, общесистемное и специализированное программное обеспечение, виртуальную инфраструктуру.

При выборе серверного и хостового программного обеспечения должны учитываться требования по импортозамещению и совместимости программного обеспечения между собой.

Подсистема хранения данных должна включать следующие модули:

- Система хранения закрытого контура;
- Система хранения открытого контура;
- Система хранения средств технической защиты;
- Система хранения инженерных систем здания.

Для краткосрочного и долгосрочного хранения данных, а также для хранения резервных копий должны использоваться ресурсы, размещаемых в ЦОД.

Архивные данные должны размещаться на ресурсах в удалённом доверенном ЦОД.

Подсистема инженерной инфраструктуры для ИТ должна включать следующие модули:

- Серверные помещения/коммуникационные: монтажные конструктивы;
- Серверные помещения/коммуникационные: системы обеспечения температурно-влажностного режима;
- Серверные помещения/коммуникационные: системы пожаротушения;
- Серверные помещения/коммуникационные: электроснабжение;

- Серверные помещения/коммуникационные: системы контроля доступа, видеонаблюдения, сигнализации.

Требования по количеству, составу, размещению и электропотреблению серверных шкафов будет приведены на этапе технического проектирования.

Подсистема защиты информации должна включать следующие модули:

- Средства обеспечения защиты информации от НСД;
- Средства физической защиты информации.

Уточнение требований необходимо провести в рамках ЧТЗ.

Функциональные подсистемы должны включать в себя:

- Прикладные подсистемы образовательного учреждения (ОУ);
- Технические подсистемы

Прикладные подсистемы образовательного учреждения (ОУ) должны включать в себя:

- Подсистема поддержки образовательного процесса;
- Подсистема административного блока ОУ;
- Подсистема цифровой лаборатории (FabLab);
- Подсистема социального блока ОУ;
- Подсистема электронной библиотеки/цифрового контента;
- Подсистема «студия звукозаписи»;
- Подсистема «актовый зал»;
- Подсистема «арена киберспорта»;
- Подсистема NFT «невзаимозаменяемый токен»

Подсистема поддержки образовательного процесса должна включать следующие модули:

- Электронный дневник
- Модуль "Домашнее задание"
- Личный кабинета родителя\ученика
- Функциональный модуль "Расписание"
- Тесты с проверкой учителя\автопроверкой
- Внеурочная деятельность

Необходимо разработать отдельные ЧТЗ с требованиями к помещениям для следующих подсистем:

- Подсистема цифровой лаборатории (FabLab);
- Подсистема «студия звукозаписи»;
- Подсистема «актовый зал»; (задание на виртуализацию у платформ икса)
- Подсистема «арена киберспорта»;

Технические подсистемы должны включать в себя:

- Подсистема инфраструктурных сервисов;
- Подсистема мониторинга и управления инженерными системами;

	Требования к функциональным подсистемам и модулям	• Подсистема мониторинга и управления средствами защиты информации; • Подсистема мониторинга и управления средствами передачи данных; • Подсистема диспетчеризации цифровых слоев BIM; • Подсистема мониторинга и управления средствами вычислительными ресурсами; • Подсистема позиционирования учащихся и персонала на территории учебного заведения. Подсистема мониторинга и управления инженерными системами АСУД, АСТУЭ, СКУД/СОТС, СОТ и АПС должны образовывать единую экосистему, обеспечивающую взаимный обмен данными для обеспечения комфорта пребывания на территории учебного учреждения, возможностей эффективной эксплуатации, обеспечения энергоэффективности и возможности дальнейшего расширения предоставляемых учреждением цифровых сервисов. Уточнение требований необходимо провести в рамках ЧТЗ. Основанием для разработки подсистемы защиты информации (далее – ПСЗИ) должны являться нормативные правовые акты Российской Федерации, методические документы ФСТЭК России, ФСБ России, в сфере обеспечения безопасности конфиденциальной информации, в том числе персональных данных, а также методические документы Минобрнауки России и Минкомсвязи России: • Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; • Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»; • Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»; • Федеральный закон от 28 июля 2012 г. № 139-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации»; • Федеральный закон от 2 июля 2013 г. № 187-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях»; • Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей Международного информационного обмена»; • Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Требования к защите персональных данных при их обработке в информационных системах персональных данных»; • Постановление Правительства Российской Федерации от 10 июля 2013 г. № 582 «Правила размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети «Интернет» и обновления информации об образовательной организации»; • Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»; • «Методика оценки угроз безопасности информации» утверждена ФСТЭК России 5 февраля 2021 г.; • Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), введено приказом ФСБ России от 9 февраля 2005 г. № 66; • «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утвержденные руководством 8 Центра ФСБ России 21 февраля 2008 г., №149/54-144; • Приказ ФСБ России № 378 от 10.07.2014 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством

	Требования к подсистеме защиты информации	Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»; • Письмо Министерства образования и науки РФ от 25.12.13 № НТ1338/08; • Письмо Минобрнауки России от 14.05.2018 N 08-1184 «О направлении информации» (вместе с «Методическими рекомендациями о размещении на информационных стендах, официальных интернет-сайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление в сфере образования, информации о безопасном поведении и использовании сети «Интернет»); • Приказ Минкомсвязи России от 16.06.2014 № 161 «Об утверждении требований к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию». • Распоряжение Правительства РФ от 02.12.2015 № 2471-р. • Правила подключения общеобразовательных учреждений к единой системе контент-фильтрации доступа к сети Интернет, реализованной Министерством образования и науки Российской Федерации от 11 мая 2011 года № АФ-12/07 вн. • Методические рекомендации по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования (утв. Министерством просвещения РФ, Министерством цифрового развития, связи и массовых коммуникаций РФ, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций 16 мая 2019 г.). • Методические рекомендации по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования (далее – методические рекомендации) разработаны в рамках реализации пункта 7 плана мероприятий по реализации Концепции информационной безопасности детей на 2018-2020 годы, утверждённого приказом Минкомсвязи России от 27 февраля 2018 г. № 88. • Методические рекомендации по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, направленные Минобрнауки России письмом от 28.04.2014 № ДЛ-115/03. • ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью; • ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения; • ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения; • ГОСТ Р 51583-2000 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения; • ГОСТ Р 50922-2006 Защита информации. Основные термины и определения; • ГОСТ Р ИСО/МЭК 13335 Информационная технология. Методы и средства обеспечения безопасности. Важным требованием обеспечения деятельности образовательного учреждения является поддержание высокого уровня информационной безопасности. Помимо защиты обрабатываемых персональных данных учащихся, преподавательского состава и обслуживающего персонала школы, а также информации ограниченного распространения (обучающие программы, базы данных, библиотеки, другая структурированная информация, применяемая для обеспечения учебного процесса, а также защищаемая законом интеллектуальная собственность), необходимо оградить учащихся от любых проявлений пропаганды и манипуляций. Информационная безопасность образовательного учреждения должна представлять собой комплекс мер различного характера, направленных на реализацию двух основных целей. Первой целью является защита персональных данных и информационного пространства от несанкционированных вмешательств, хищения информации и изменения конфигурации со стороны третьих лиц. Вторая цель – защита учащихся от любых видов пропаганды, рекламы, запрещенной законом информации. Выбор и реализация методов и способов защиты информации в информационной системе, созданной в рамках проекта должна осуществляться на основе актуальных угроз безопасности, оценка которых определяется в Модели угроз безопасности, а также в зависимости от уровня защищенности ИСПДн. Функционирование ПСЗИ должно быть обеспечено комплектом организационно – распорядительной и эксплуатационной документацией в соответствии с требованиями законодательства Российской Федерации, а также методических документов ФСБ России и ФСТЭК России в сфере обеспечения безопасности конфиденциальной информации, в том числе персональных данных.

ПСЗИ должна быть централизованной. Любые действия, связанные с внесением изменений в базовую конфигурацию, управление (администрирование) системой должны осуществляться доверенными лицами с разрешения и под контролем ответственного за обеспечение безопасности информации.

В ПСЗИ должны быть реализованы следующие модули защиты информации, которые могут уточняться на этапе технического проектирования:

- идентификации и аутентификации субъектов доступа и объектов доступа;
- управления доступом субъектов доступа к объектам доступа;
- защиты машинных носителей ПДн;
- регистрации событий безопасности;
- антивирусной защиты;
- контроля (анализа) защищенности ИС;
- обеспечения целостности информационной системы;
- обеспечения доступности ИС;
- защиты среды виртуализации;
- защиты технических средств
- защиты информационной системы, ее средств, систем связи и передачи данных;
- межсетевого экранирования;
- выявления инцидентов и реагирования на них;
- управления конфигурацией ИС и ПСЗИ.

ПСЗИ должна поддерживать следующие режимы функционирования:

- основной режим, в котором все подсистемы выполняет свои функции в полном объеме;
- режим обслуживания, в котором одна или несколько подсистем не выполняют свои функции.

В основном режиме функционирования ПСЗИ должна обеспечивать непрерывную защиту информации, выполнять сбор, обработку и хранение событий безопасности.

В режиме обслуживания должна обеспечивать проведение следующих работ:

- техническое обслуживание средств защиты информации (СрЗИ) и средств криптографической защиты информации (СКЗИ);
- модернизацию программных и программно-аппаратных СрЗИ и СКЗИ;
- устранение аварийных случаев и инцидентов безопасности.

Для обеспечения высокой надежности выполнения ПСЗИ своих функций, периодически должны проводиться мероприятия контроля эффективности, включающие в себя:

- проверку знаний пользователей и персонала своих должностных обязанностей в области обеспечения безопасности обрабатываемой информации;
- тестирование СрЗИ и СКЗИ.

ПСЗИ должна быть гибкой, иметь возможность выполнять свои функции при изменении структурно-функциональных характеристик ИТ-инфраструктуры в объеме, предусмотренном эксплуатационной документацией.

ПСЗИ должна обеспечивать адаптацию к изменениям в ИС за счет:

- своевременного внесения изменений в организационно-распорядительную документацию при изменении характеристик обрабатываемой информации, состава персонала, федерального законодательства и иных нормативно-правовых актов в области обеспечения безопасности информации, структурно-функциональных характеристик в рамках эксплуатационной документации на ИС;
- своевременного управления (администрирования) ИС;
- модернизации программных и программно-аппаратных СрЗИ и СКЗИ в соответствии с вновь выявленными угрозами.

Экономический эффект от создания ПСЗИ должен проявляться в снижении вероятной величины материального и морального ущерба, вызванной снижением уровня информационной безопасности информации в ИС.

Требования к средствам физической защиты объекта

Под охраной объекта подразумевается комплекс мер, направленных на своевременное выявление угроз и предотвращение нападения на объект, совершения террористического акта, других противоправных посягательств в т.ч. экстремистского характера, а также возникновения чрезвычайных ситуаций.

Система обеспечения комплексной безопасности объекта это совокупность предусмотренных законодательством мер и мероприятий персонала объекта, осуществляемых под руководством органов управления образованием и органов местного самоуправления во взаимодействии с правоохранительными структурами, вспомогательными службами и общественными организациями (формированиями), с целью обеспечения его безопасного функционирования, а также готовности сотрудников и учащихся к рациональным действиям в чрезвычайных ситуациях. Целью, процессом и результатом реализации указанных мер и мероприятий является комплексная безопасность объекта как его состояние защищенности от реальных и прогнозируемых угроз социального, техногенного и природного характера.

Виды, система и порядок охраны объектов, в том числе школ, регулируются федеральными законами от 14.04.1999г. № 77-ФЗ «О ведомственной охране», от 11 марта 1992г. № 2487-1 «О частной детективной и охранной деятельности в Российской Федерации», постановлениями Правительства Российской Федерации от 04.04.2005 г. № 179 «Вопросы негосударственной (частной) охранной и негосударственной (частной) сыскной деятельности», руководящим документом МВД РФ РД 78.36.003-2002 «Инженерно-техническая укрепленность».

В соответствии с требованиями Закона РФ «О безопасности» от 05.03.1992 N 2446-1 на объекте должно обеспечиваться поддержание безопасного состояния, предотвращение, обнаружение и ликвидация угроз жизни, здоровью, среде обитания, имуществу и информации за счет внедрения СОТ, СКУД, СОТС, ССОИ, АПС, АПЗ, СОУЭ. Основные решения должны отвечать требованием следующих нормативных документов:

Постановление российского Правительства № 1006 «Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства просвещения Российской Федерации, относящихся к сфере деятельности Министерства просвещения Российской Федерации, и формы паспорта безопасности этих объектов (территорий)»;

Минпросвещения России от 28.01.2020 № ВБ85/12 «О направлении методических рекомендаций» (вместе с Методическими рекомендациями Организация деятельности по обеспечению антитеррористической защищенности объектов (территорий) Министерства просвещения Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства просвещения Российской Федерации);

Письмо Минпросвещения России от 11 мая 2021 г. № СК-123/07 с рекомендациями по организации действий в кризисной ситуации для участников образовательных отношений.

ГОСТ Р 58485-2019. «Обеспечение безопасности образовательных организаций. Оказание охранных услуг на объектах дошкольных, общеобразовательных и профессиональных образовательных организаций. Общие требования»;

ГОСТ Р 52551 «Системы охраны и безопасности. Термины и определения»;

ГОСТ Р 51558-2014 «Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний»;

ГОСТ Р 51241-2008 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний»;

ГОСТ Р 50776-95 «Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 4. Руководство по проектированию, монтажу и техническому обслуживанию»;

ГОСТ Р 53704-2009 «Системы безопасности комплексные и интегрированные. Общие технические требования»;

ГОСТ Р 52436-2005 «Приборы приемно-контрольные охранной и охранно-пожарной сигнализации. Классификация. Общие технические требования и методы испытаний»;

РД 78.36.003-2002. «Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств»;

РД 78.36.006-2005 «Выбор и применение технических средств охранной, тревожной сигнализации и средств инженерно-технической укрепленности для оборудования объектов»;

РД 78.36.004-2005 «Рекомендации по техническому надзору за выполнением проектных, монтажных и пусконаладочных работ по оборудованию объектов техническими средствами охраны»;

РД 78.145-93 «Системы и комплексы охранной, пожарной и охранно-пожарной сигнализации. Правила производства и приемки работ»;

РД 78.36.002-99 «Технические средства систем безопасности объектов. Обозначения условные графические элементов систем»;