ТРЕБОВАНИЯ БЕЗОПАСНОСТИ ЭОС ВУЗА

Дудников С.А., к.т.н., доцент

Вербицкий А.С., к.т.н., доцент

МГВОКУ, г. Москва, Россия

Вербицкий А.А.,студент

НИУ МИЭТ, г. Москва, Россия

Аннотация. В статье рассматриваются вопросы обеспечения информационной безопасности электронной образовательной среды (ЭОС) вуза. Охарактеризованы основные объекты защиты и угрозы, влияющие на конфиденциальность персональных данных, целостность учебных материалов и результатов аттестации, доступность образовательных сервисов. Раскрыта необходимость комплексного применения технических и организационных мер защиты на всех этапах жизненного цикла ЭОС. Особое внимание уделено безопасности модульной архитектуры, согласованному управлению доступом и защите межмодульного обмена данными.

Ключевые слова: электронная образовательная среда, информационная безопасность, объекты защиты, угрозы безопасности, модульная архитектура.

Электронная образовательная среда (ЭОС) вуза представляет собой целостное цифровое пространство, в котором соединяются учебные материалы, инструменты взаимодействия участников образовательного процесса и сервисы управления обучением. Через нее обеспечивается доступ к расписанию, курсам, заданиям, материалам лекций, результатам текущего контроля и итоговой аттестации. Она может применяться при традиционном обучении, в дистанционном формате и в смешанных моделях, когда часть занятий проходит очно, а часть – с использованием онлайн-инструментов. Внедрение электронной образовательной среды упрощает обмен информацией между обучающимися, преподавателями и административными подразделениями, делает учебный процесс более прозрачным и позволяет принимать управленческие решения на основе сведений об успеваемости, активности обучающихся и ходе реализации дисциплин.

Защита электронной образовательной среды и содержащихся в ней персональных данных необходима потому, что от неё зависят конфиденциальность информации, достоверность результатов обучения и способность университета бесперебойно оказывать образовательные услуги. Если защита выстроена недостаточно, возникают риски постороннего вмешательства, утечек, подмены данных и утраты материалов. Подобные нарушения способны затронуть права обучающихся и сотрудников, затруднить организацию учебного процесса и нанести ущерб репутации вуза. Поэтому безопасность должна обеспечиваться не отдельными разовыми мерами, а системой технических решений и организационных процедур, которые дополняют друг друга.

Особое место среди защищаемых объектов занимают учётные записи пользователей. Именно они позволяют идентифицировать обучающихся, преподавателей, сотрудников и администраторов, а также определяют, какие именно ресурсы и действия доступны каждому участнику. С учётной записью связаны средства подтверждения личности, назначенные роли и полномочия. Если данные входа становятся известными постороннему лицу или злоумышленнику, появляется возможность действовать от имени законного пользователя. В этом случае последствия могут распространяться не только на один сервис, но и на все ресурсы, к которым у пользователя был открыт доступ.

Сведения личного характера, относящиеся к обучающимся, преподавателям и работникам вуза, должны быть защищены от несанкционированного раскрытия, изменения и неправомерного использования. Отдельную категорию защищаемой информации составляют учебные материалы: электронные курсы, лекции, методические разработки, задания, тестовые материалы и вспомогательные ресурсы. Их следует оберегать от повреждения, удаления и распространения за пределами установленного круга пользователей. Особенно важно сохранить целостность результатов аттестации, к которым относятся оценки, экзаменационные ведомости, зачётные результаты и загруженные работы. От достоверности этих данных зависит корректность решений о том, насколько успешно освоена образовательная программа.

К числу основных угроз для электронной образовательной среды обычно относят несанкционированный доступ, утечки, подмену или уничтожение данных, действие вредоносных программ, нарушения доступности сервисов и ошибочные действия пользователей. Каждый из этих факторов способен привести к серьёзным последствиям как сам по себе, так и в сочетании с другими неблагоприятными обстоятельствами.

Несанкционированный доступ означает, что лицо получает информацию или использует функциональные возможности среды сверх предоставленных ему прав. Такое может происходить из-за компрометации средств входа, использования уязвимостей программного обеспечения или неправильной настройки разграничения полномочий. Источник угрозы не обязательно находится вне университета. Им может быть и пользователь, который обладает законным доступом, но выполняет действия, выходящие за пределы его роли или служебных задач.

Утечка информации проявляется в том, что данные становятся доступны тем, кто не должен с ними знакомиться. Подмена данных нарушает их достоверность: например, могут быть изменены оценки, отредактированы задания или искажены сведения о выполнении заданий. Уничтожение информации означает потерю материалов, записей или документов, необходимых для учебного процесса. Похожие последствия могут наступать не только из-за злого умысла, но и из-за случайных действий, технических отказов и сбоев. Поэтому защита должна включать ограничение доступа, регистрацию важных операций, контроль изменений и регулярное создание проверяемых резервных копий.

Вредоносные программы представляют опасность как для устройств пользователей, так и для серверной части электронной образовательной среды. Их действие может сопровождаться кражей данных для входа, скрытным изменением файлов, шифрованием информации и нарушением работоспособности приложений. Источником заражения нередко становятся вложения в электронных письмах, загружаемые файлы или программные компоненты, полученные из непроверенных источников.

Атаки на доступность направлены на то, чтобы ограничить или полностью прекратить работу образовательных сервисов. Иногда это достигается за счёт создания чрезмерной нагрузки на систему. Особенно ощутимыми такие сбои становятся в периоды дистанционных занятий, сдачи работ и проведения контрольных мероприятий. Вместе с тем перегрузка может возникать и без внешнего нападения, например, когда большое число обучающихся одновременно обращаются к одному и тому же сервису.

Ошибки пользователей тоже способны создавать уязвимости и нарушать нормальную работу среды. К ним относятся случайное удаление материалов, разглашение паролей, пересылка сведений не тому адресату и неверное назначение прав доступа. Чтобы снизить вероятность таких ситуаций, следует делать интерфейсы понятными, применять безопасные настройки по умолчанию и регулярно обучать обучающихся, преподавателей и сотрудников правилам работы с цифровыми системами.

Подключение внешних образовательных платформ может расширять возможности электронной среды, однако одновременно увеличивает число компонентов, от которых зависит общая безопасность. Передача данных между внутренними и внешними системами создаёт риски избыточного раскрытия информации, нарушения согласованности записей и компрометации интерфейсов взаимодействия. Если внешний сервис становится недоступным, это может блокировать учебные операции, которые были с ним связаны. Поэтому при интеграции нужно заранее определять, какие именно данные передаются, какие полномочия получает внешняя система и каким образом действовать при сбоях.

Удалённый доступ означает, что пользователи работают с системами вуза через устройства и сети, находящиеся вне прямой зоны контроля университета. Устаревшее программное обеспечение, заражённые компьютеры и небезопасное хранение данных для входа повышают вероятность компрометации. Для уменьшения таких рисков используются защищённые каналы связи, многофакторная аутентификация, управление сеансами и отслеживание подозрительной активности. При этом меры безопасности не должны превращаться в непреодолимый барьер для добросовестных пользователей, которым необходимо получать доступ к учебным материалам.

Если электронная образовательная среда построена по модульному принципу, каждый её компонент следует рассматривать не только как самостоятельную функциональную часть, но и как отдельный объект защиты. Защищать нужно те операции, которые выполняет модуль, данные, которые он обрабатывает и хранит, а также настройки и интерфейсы, через которые он взаимодействует с другими частями системы. Набор мер защиты определяется назначением модуля, важностью информации и тем, к каким последствиям может привести нарушение конфиденциальности, целостности или доступности.

В рамках каждого модуля должны проверяться полномочия пользователя перед выполнением операций, разграничиваться доступ к данным, контролироваться входная информация и регистрироваться значимые действия. Наличие единого входа не означает, что пользователю автоматически разрешены все функции среды. Даже если подтверждена личность, проверка прав должна выполняться и на уровне конкретного компонента. Поэтому общие механизмы безопасности нужно сочетать со специальными мерами, например, с контролем изменения оценок, проверкой загружаемых файлов или ограничением доступа к журналу действий.

Тесное взаимодействие компонентов требует защиты не только внутри отдельных модулей, но и на границах между ними. Обмен данными должен происходить с проверкой подлинности участников, ограничением прав и контролем целостности передаваемой информации. Компрометация одного элемента не должна приводить к тому, что нарушитель получает доступ ко всей среде. В результате безопасность модульной системы складывается из согласованных общих и локальных мер, которые продолжают действовать при подключении новых компонентов, обновлении существующих и замене отдельных элементов.

Исходя из этого, к базовым требованиям безопасности электронной образовательной среды целесообразно отнести:

идентификацию, аутентификацию и управление доступом;

защиту персональных и образовательных данных;

безопасность приложений и интеграций;

защиту инфраструктуры;

обеспечение достоверности результатов обучения;

мониторинг и реагирование на инциденты;

непрерывность работы и восстановление;

организационные требования и контроль.

Требование, касающееся идентификации, аутентификации и управления доступом, направлено на то, чтобы точно устанавливать пользователя и предоставлять ему только те полномочия, которые нужны для выполнения учебных или служебных функций. Идентификация позволяет отличить одного пользователя от другого по уникальному признаку. Аутентификация подтверждает, что пользователь действительно владеет заявленной учётной записью. Управление доступом определяет, какие действия ему разрешены в системе. Для обучающихся, преподавателей, сотрудников и администраторов должны создаваться персональные учётные записи, жизненный цикл которых поддаётся управлению: их можно создать, изменить, временно заблокировать или отключить. Единый вход удобен для согласованного доступа к подключённым сервисам, но он не заменяет проверку прав внутри каждого модуля. Разрешения могут зависеть не только от роли, но и от принадлежности пользователя к группе, дисциплине, подразделению или конкретному процессу. Для привилегированных учётных записей и особенно чувствительных операций следует применять усиленную аутентификацию, включая многофакторную.

Конкретизация этого требования включает правила управления паролями и сессиями, условия блокировки при подозрительных попытках входа, порядок назначения и пересмотра полномочий. Отдельно нужно урегулировать использование технических учётных записей, которые применяются для взаимодействия приложений между собой. Проверять можно сроки прекращения доступа после изменения статуса пользователя, периодичность пересмотра прав и долю привилегированных учётных записей, переведённых на многофакторную аутентификацию.

Требование защиты персональных и образовательных данных предполагает, что конфиденциальность, целостность и доступность информации обеспечиваются на всех этапах её существования: от получения и использования до архивирования и удаления. К защищаемым объектам относятся сведения о обучающихся и сотрудниках, учебные работы, оценки, результаты контроля, записи занятий, сообщения и иные данные, циркулирующие в электронной среде. Разные категории информации могут требовать разного уровня защиты.

Для каждого типа данных следует определить цель обработки, допустимый объём, место хранения, ответственного владельца, круг пользователей и срок хранения. Система не должна собирать сведения, которые не нужны для заявленных задач. Доступ ограничивается полномочиями пользователей, а передача данных выполняется по защищённым каналам. Вопрос о необходимости шифрования при хранении решается с учётом чувствительности сведений и условий их обработки; при этом управление ключами должно исключать их несанкционированное раскрытие.

Защите подлежат не только основные базы данных, но и выгрузки, резервные копии, временные файлы, а также данные, находящиеся на устройствах пользователей. Если информация используется для аналитики или тестирования, желательно применять обезличенные или искусственно созданные данные, когда это позволяет решить задачу. В качестве критериев проверки могут использоваться соблюдение сроков хранения, отсутствие избыточных прав, защищённость каналов передачи и возможность контролируемого удаления данных из соответствующих хранилищ.

Требование безопасности приложений и интеграций относится к программным

компонентам среды и способам их взаимодействия. Портал, система управления обучением, библиотечные сервисы, средства тестирования и другие приложения должны препятствовать несанкционированным операциям, утечке данных и искажению информации. Безопасность следует закладывать на этапах разработки, настройки, внедрения и дальнейшего обновления программных решений.

На уровне приложений нужно проверять входные данные, контролировать полномочия на серверной стороне, безопасно обрабатывать загружаемые файлы и не допускать раскрытия служебной информации через сообщения об ошибках. Для программных интерфейсов следует устанавливать допустимые операции, правила аутентификации, ограничения на интенсивность запросов и проверку передаваемых данных. Каждая интеграция должна получать минимально необходимые полномочия: подключение внешнего сервиса не должно означать доступ ко всей среде без ограничений.

Особое внимание должно уделяться управлению программными зависимостями, своевременному устранению уязвимостей и безопасному хранению паролей, токенов и ключей. Обмен данными должен учитывать возможность повторной отправки сообщений, частичных сбоев и получения некорректных сведений. Проверяемыми характеристиками могут быть сроки устранения уязвимостей разной степени критичности, охват интерфейсов проверками безопасности и наличие документированных правил взаимодействия компонентов.

Требование защиты инфраструктуры распространяется на серверы, сети, системы хранения, средства виртуализации, облачные ресурсы и рабочие места администраторов, обеспечивающие работу электронной образовательной среды. Цель

состоит в том, чтобы предотвратить несанкционированный доступ к вычислительным ресурсам, изменение конфигураций, распространение вредоносного программного обеспечения и нарушение работы сервисов.

Инфраструктуру следует разделять на зоны с разным уровнем доверия и назначением. Пользовательские сервисы, базы данных, средства администрирования и резервного копирования не должны иметь необоснованных прямых связей. Для серверов и сетевого оборудования нужно применять безопасные конфигурации, отключать неиспользуемые службы, ограничивать административный доступ и обеспечивать управляемое обновление. Среды разработки и тестирования должны быть отделены от рабочей среды.

Кроме того, следует предусматривать физическую защиту оборудования, контроль доступа в серверные помещения и противодействие сетевым атакам. Если часть среды размещается в облаке, необходимо чётко определить, за что отвечает вуз, а за что – поставщик услуг. Показателями соответствия могут служить полнота учёта объектов инфраструктуры, соблюдение утверждённых конфигураций, своевременная установка обновлений и отсутствие недопустимых сетевых соединений.

Требование обеспечения достоверности результатов обучения направлено на то, чтобы сведения о выполненных работах, оценках и аттестации оставались корректными, контролируемыми и защищёнными. Электронная среда должна позволять установить, кем и когда была представлена работа, кто её оценивал и на каком основании изменялся результат. При этом сама по себе фиксация действий учётной записи не всегда доказывает, что задание выполнено лично определённым обучающимся.

Для обеспечения достоверности необходимо разграничивать полномочия обучающихся, преподавателей и сотрудников, отвечающих за учёт результатов. Если оценка изменяется, предыдущее значение должно сохраняться вместе с временем операции, идентификатором исполнителя и основанием корректировки. Для важных документов могут применяться процедуры подтверждения и утверждения. Передача результатов между учебной системой и административными системами должна исключать незаметную подмену, потерю и ошибочное сопоставление записей.

Требование мониторинга и реагирования на инциденты предполагает наблюдение за значимыми событиями безопасности и заранее установленный порядок действий при выявлении нарушений. Мониторинг должен охватывать попытки входа, изменения полномочий, административные операции, обращения к защищаемым данным, изменение результатов обучения и сбои интеграций.

Журналы событий должны содержать достаточно информации для последующего анализа: время, источник, субъекта действия, объект обращения и результат операции. Чтобы сопоставлять события из разных модулей, необходимо синхронизировать время. Сами журналы следует защищать от несанкционированного изменения и просмотра, но в них не должны попадать пароли и избыточные персональные сведения.

Реагирование включает регистрацию инцидента, оценку его значимости, ограничение последствий, сохранение доказательств, устранение причины и последующую проверку восстановления нормальной работы. У ответственных сотрудников должны быть

заранее определены полномочия и каналы взаимодействия. Измеримыми характеристиками могут быть время обнаружения инцидента, время уведомления, время локализации, охват компонентов мониторингом и срок хранения журналов.

Требование непрерывности работы и восстановления направлено на сохранение наиболее важных образовательных процессов при технических сбоях, ошибках, атаках и пиковых нагрузках. Поскольку разные модули имеют разную критичность, для каждого из них следует определить допустимое время перерыва и приоритет восстановления. Например, отказ системы проведения аттестации во время экзамена значительно серьёзнее, чем временная недоступность вспомогательной отчётности.

Ключевыми характеристиками здесь являются целевое время восстановления и допустимый период потери данных. На их основе выбираются периодичность резервного копирования, способы резервирования оборудования и каналов связи, а также порядок восстановления зависимых сервисов. Резервные копии также должны быть защищены от изменения или уничтожения в случае компрометации основной среды.

Сам факт наличия резервных копий ещё не доказывает, что восстановление возможно. Поэтому следует регулярно проводить испытания восстановление данных и сервисов, нагрузочное тестирование и актуализацию аварийных инструкций. Для пользователей с нестабильной связью могут предусматриваться ограниченные автономные сценарии с последующей безопасной синхронизацией. Проверяемыми показателями служат фактическая доступность сервисов, достигнутые значения целевого времени восстановления и допустимого периода потери данных, успешность восстановления и

устойчивость к расчётной нагрузке.

Организационные требования и контроль задают управленческие условия, без которых технические меры не дают устойчивого эффекта. В вузе должны быть определены владельцы информационных ресурсов, ответственные за эксплуатацию модулей, администраторы и сотрудники, выполняющие контрольные функции. Распределение обязанностей нужно строить так, чтобы критически важные процессы не оставались без ответственного лица.

Организационное обеспечение включает правила предоставления доступа, обработки информации, подключения внешних сервисов, внесения изменений и действий при инцидентах. Необходимо обучать пользователей безопасной работе, инструктировать администраторов и контролировать деятельность подрядчиков. Изменения архитектуры и состава интеграций должны сопровождаться оценкой рисков и пересмотром действующих мер защиты.

Контроль предполагает регулярную проверку выполнения требований, анализ выявленных недостатков и отслеживание корректирующих действий. Для каждого требования нужно фиксировать объект применения, ответственного, способ реализации и подтверждающие материалы: результаты испытаний, журналы, настройки или утверждённые регламенты. В качестве критериев оценки могут выступать актуальность документации, охват пользователей обучением, периодичность проверок и своевременность устранения нарушений.

Каждое базовое требование безопасности электронной образовательной среды является обобщённым положением, которое на этапе проектирования нужно конкретизировать для отдельных модулей, ресурсов и процессов. Такая конкретизация предполагает определение защитных свойств, качественных и количественных характеристик, а также технических и организационных мер, необходимых для защиты конкретного элемента. При этом учитываются его назначение, состав обрабатываемых данных, категории пользователей, характер взаимодействия с другими компонентами и потенциальные последствия реализации угроз.

Например, общее требование разграничения доступа раскрывается через набор ролей, перечень разрешённых операций, проверку полномочий при обращении к ресурсам и порядок пересмотра назначенных прав. Требование доступности конкретизируется через допустимую длительность перерыва, сроки восстановления сервисов, периодичность резервного копирования и порядок проверки восстановления данных. В результате общие формулировки превращаются в требования, по которым можно понять, какими свойствами должен обладать компонент, какие действия необходимы для его защиты и какие критерии позволяют оценить результат.

Формализованное требование должно быть однозначным, практически реализуемым и проверяемым. Для него следует определить объект применения, условия выполнения, ответственных и способ подтверждения соответствия. В модульной электронной образовательной среде требования должны распространяться как на внутренние функции и данные каждого компонента, так и на интерфейсы обмена между ними. Если такие требования выполняются согласованно, обеспечивается не только защита отдельных элементов, но и устойчивость образовательной среды в целом.

Таким образом, безопасность электронной образовательной среды вуза представляет собой непрерывный процесс, который объединяет техническую защиту, организационное управление и повышение осведомлённости пользователей. Эффективность этого процесса определяется не только наличием отдельных средств защиты, но и тем, насколько последовательно они применяются, как часто выполняется контроль и насколько вуз готов действовать при инцидентах. При соблюдении этих условий можно развивать функциональные возможности электронной образовательной среды, сохраняя защищённость информации и устойчивость основных образовательных процессов.