Проблемы информационной безопасности в распределенной информационной образовательной среде

Минзов А.С., Токарева Н.А., Черемисина Е.Н.

ИСАУ, университет «Дубна»

NEC’2019, Черногория

ИНСТИТУТ СИСТЕМНОГО АНАЛИЗА И УПРАВЛЕНИЯ

Содержание

- ✓ Введение в проблему
- ✓ Типовые уязвимости распределенной информационной образовательной среды (анализ и предложения по механизмам защиты и создания доверенной среды безопасности)
- ✓ Выводы

Чем сложнее информационная система, тем больше она имеет уязвимостей и тем сложнее защищать информацию в ней.

Резкое увеличение пропускных возможностей каналов связи (внедрение протоколов 5g) и технических характеристик вычислительной техники, а также реализация государственной программы цифровой экономики создали условия для массового внедрения в образовательные процессы учебных заведений систем электронного обучения.

Это привело к создания распределенной неоднородной по формам, содержанию и системе управления информационной и образовательной среды.

Анализ проблемы

Новая информационная образовательная среда позволяет использовать образовательные ресурсы:

- различных субъектов от федерального и региональных уровней,
- образовательных учреждений и центров дистанционного обучения,
- информационных ресурсов различных хозяйствующих субъектов,
- фондов и электронных библиотек,
- информационных ресурсов социальных сетей,
- электронных архивов,
- частных информационных ресурсов физических лиц
- и других источников информации

- С появлением и массовым применением облачных сред появилась возможность виртуального моделирования технических систем, что значительно расширило возможности дистанционных технологий, а внедрение в различные технические системы сетевых интерфейсов позволило включать в образовательные процессы научно – исследовательские проекты с удаленным управлением оборудованием и удаленным экспериментом.
- По существу, в настоящее время создана ***распределенная информационная образовательная среда (РИОС) с децентрализованным управлением со слабой обратной связью*** .
- Централизованное управление РИОС обеспечивается только на федеральном уровне (выполнение определенных требований к метафизическому описанию электронных ресурсов)

- Все остальные информационные и образовательные ресурсы имеют ссылочный характер и формируются по частным требованиям к формам представления электронных образовательных ресурсов различных организаций.

При этом:

- Даже центральный образовательный портал ***http://window.edu.ru*** не обеспечивает защиту информации и системы управления порталом по протоколу *https.* Это **не создает доверительную ср**еду и для образовательных учреждений, так как информационные ресурсы этого портала остаются незащищенными.

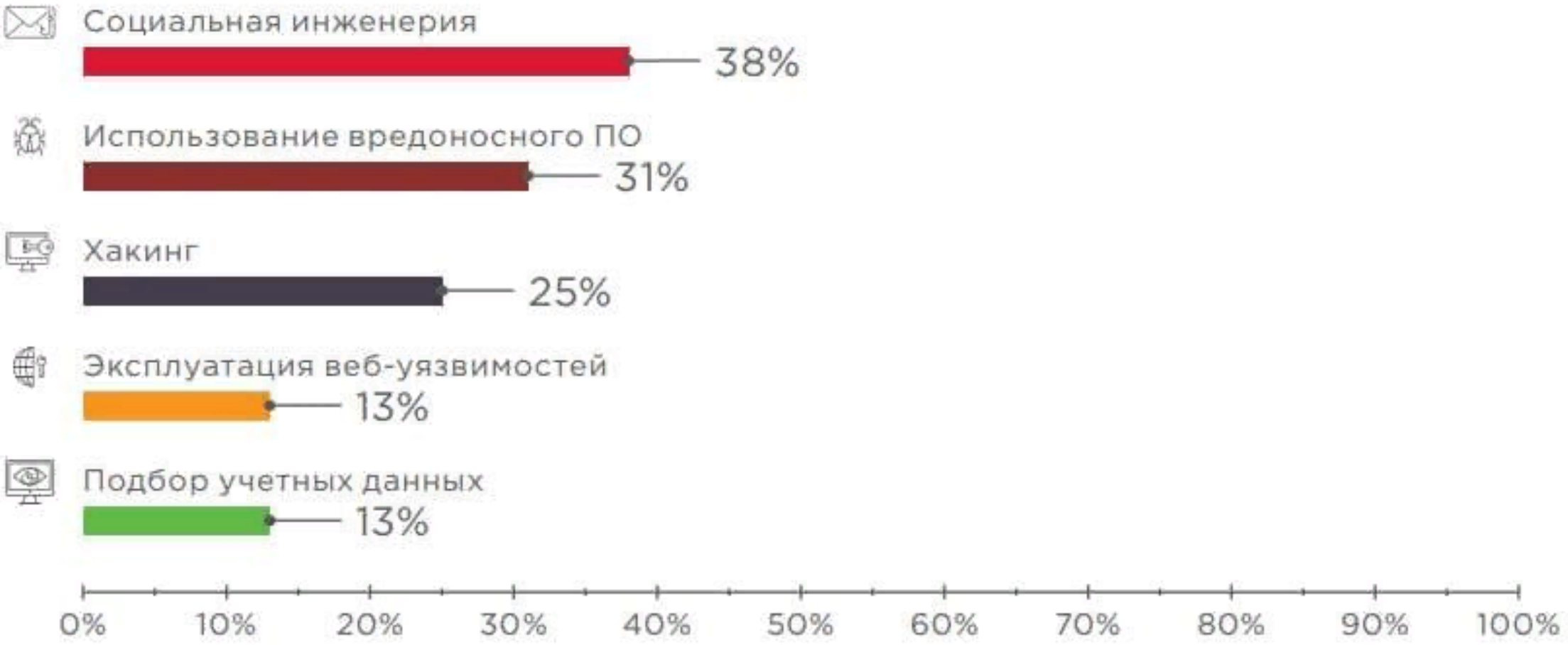
- Обратная связь по мониторингу изменений информационных ресурсов, контролю доступа к ним, оценке соответствия их требованиям к форме и содержанию практически не предусматривается. Это **не позволяет контролировать их качество и актуальность**.
- На региональном уровне **требования к информационной безопасности практически отсутствуют**.
- Образовательные и информационные ресурсы образовательных учреждений федеральных и национальных исследовательских университетов, отдельных вузов, центров дистанционного обучения и ресурсов социальных сетей **не носят универсальный характер**, встроены в свои информационные системы дистанционного обучения и чаще всего **носят закрытый или коммерческий характер**.

Нормативное обеспечение

- С 2011 года начата работа по стандартизации разработки, внедрения и сопровождения электронный образовательных ресурсов (ЭОР). Результаты этой работы реализованы в стандартах ГОСТР 57723- 2017, ГОСТ Р 53620-2009, ГОСТ Р 55750-2013, ГОСТ Р 55750-2013, ГОСТ Р 55751-2013, ГОСТ Р ИСО/МЭК 2382_36 – 2011.
- Однако они **носят общий характер**.. В них практически отсутствуют требования к информационной безопасности ЭОР и систем управления ими за исключением ГОСТ Р 577723-2017 , описывающему требования по безопасности электронно-библиотечных систем.
- На федеральном уровне вся **ответственность** за обеспечение безопасности, актуальности и качеству ЭОР ложится **на автора ЭОР**, а **никаких функций по контролю информационной безопасности ЭОР при его включении в реестр не проводится**.

Методы атак на образовательные учреждения (на июнь 2018 г.)

https://www.ptsecurity.com/ru-ru/research/analytics/



Наиболее значимые угрозы РИОС (по отзывам пользователей)

- Наличие вредоносного кода в загружаемом ЭОР (курсы лекций, лабораторных практикумов и заданий).
- Неактуальная (устаревшая) информация в ЭОР.
- Модифицированная (ложная и некорректная информация, которая иногда вводится искусственно). Особенно это проявляется в распространенном ресурсе Wikipedia и в открытых ресурсах центров дистанционного обучения.
- Некорректное представление математических описаний и моделей: некорректные индексы, логические выражения, использование текстовых редакторов вместо математических.

Наиболее значимые угрозы РИОС (по отзывам пользователей)

- Некорректное представление схем, графиков, диаграмм и презентаций.
- Списки использованных источников обычно существуют, но не привязаны конкретно к их заимствованиям по тексту.
- Отсутствие описание проблем, новизны, постановок нерешенных задач.
- Отсутствие научности в образовательном и информационном контенте.

Эти угрозы качественному образовательному процессу во многом связаны с отсутствием политик информационной безопасности к ЭОР и системе их менеджмента.

Типовые уязвимости РИОС и предложения по механизмам защиты

- Уязвимости РИОС, основанные на ошибках реализации портальных решений.

Требуется применения рекомендаций по снижению уязвимостей портальных решений.

- Уязвимости систем управления образовательным и информационным контентом (LMS).

Требуется расширения базы знаний по уязвимостям LMS в Банке данных угроз и уязвимостей ФСТЭК

Типовые уязвимости РИОС и предложения по механизмам защиты

- Возможность включения вредоносного кода в информационный и образовательный контент.
- Возможность включения недекларированных функций в специальное программное обеспечение РИОС.

Требуется обязательный контроля ЭОР на наличие вредоносного кода и анализ программного обеспечения на НДВ (недекларированные возможности).

Типовые уязвимости РИОС и предложения по механизмам защиты

- Отсутствие контроля действий субъектов образовательного процесса.

Защита обеспечивается настройками LMS.

- Отсутствие системы мониторинга целостности информационного и образовательного контента и механизмов его обновления.

Необходимо включение в состав ПО механизмов контроля целостности ЭОР.

Типовые уязвимости РИОС и предложения по механизмам защиты

- Отсутствие механизмов защиты интеллектуальной собственности авторов ЭОР в РИОС и контроля заимствований.
- Отсутствие единой системы требований к описанию и представлению ЭОР, в том числе в активных и интерактивных формах обучения.
- Отсутствие механизмов безопасной передачи, обмена и других форм использования ЭОР между субъектами образовательного процесса в РИОС.
- Отсутствие достаточной нормативной базы для создания, внедрения и сертификации системы информационной безопасности ЭОР.

Требуется разработать организационные мероприятия с учетом стандартов для ЭБС

Перечень уязвимостей, для устранения которых потребуются значительные усилия

- Достоверность информационных и образовательных ресурсов.

В контексте РИОС имеет несколько другой смысл, чем используемый в настоящее время в системах информационной безопасности. Достоверность (reliability): свойство соответствия предусмотренному поведению и результатам. По существу, в системах информационной безопасности мы создаем механизм достоверности по источнику информации, а не самой информации, что значительно сложнее и вряд ли может быть на этом этапе развития систем управления информационной безопасностью полностью автоматизировано.

На наш взгляд, образовательный контент должен содержать безопасную для обучаемого информацию, отражающую современное, общепринятое научное представление изучаемых вопросов и мнений.

В образовательном контенте не должно содержаться лженаучных теорий и искусственно вводимых понятий и определений, либо, если эти вопросы все же излагаются, то они должны иметь критическую форму их представления.

Формализованное описание контента должно иметь доказательную форму представления, а не аксиоматическую.

Перечень уязвимостей, для устранения которых потребуются значительные усилия

Механизм обеспечения достоверности информации в РИОС должен быть отражен в нормативной документации для разработки ЭОР и определяться ответственностью авторов, рецензентов и содержать систему мониторинга достоверности образовательного контента как при его включении в образовательный РИОС, так и в процессе его использования и обновления.

Перечень уязвимостей, для устранения которых потребуются значительные усилия

- Отсутствие механизмов защиты информации в системах удаленного управления техническими телеметрическими комплексами с сетевыми интерфейсами.

Необходимо создание системы защиты информации от сетевых угроз. Это обстоятельство предопределяет необходимость разработки систем удаленного доступа (Remote Labs) с сохранением всех основных функций по работе с каждым устройством в стенде и создание эффективной системы защиты сетей на основе WAN-соединений и портов для организации LAN соединений.

Перечень уязвимостей, для устранения которых потребуются значительные усилия

- Защита персональных данных всех участников образовательного процесса.

Требует разработки системы защиты информационных систем персональных данных. Это требует безусловного выполнения требований нормативной документации . В существующих системах это будет, как правило, 4-й уровень защищенности ПДН.

Выводы

Угрозы и уязвимости РИОС можно классифицировать на 3 группы:

- угрозы, связанные с уязвимостями портальных решений и систем управления информационным и образовательным контентом в распределенной информационной образовательной среде;
- угрозы, связанные с актуальностью, достоверностью и качеством представления контента;
- защита авторских прав ЭОР и слабая нормативная база по обеспечению информационной безопасности.

Предложены механизмы обеспечения информационной безопасности в распределенной информационной образовательной среде.

СПАСИБО ЗА ВНИМАНИЕ!