

УДК 004.056

DOI 10.52167/1609-1817-2022-120-1-134-141

Б.С. Ахметов¹, В.А. Лахно²

¹Казахский национальный педагогический университет имени Абая, Алматы, Казахстан

²Национальный университет биоресурсов и природопользования, Киев, Украина

E-mail: b.akhmetov@alt.edu.kz

ЗАЩИТА ИНФОРМАЦИИ И КИБЕРБЕЗОПАСНОСТЬ ЦИФРОВОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ УНИВЕРСИТЕТА

Аннотация. Проанализированы особенности построения безопасной с точки зрения кибернетической защиты цифровой образовательной среды современного университета (ЦОСУ) и его системы дистанционного обучения (СДО). Описана универсальная платформа «Базовый подход к защите ЦОСУ». Концептуально изложены методологические принципы построения системы обеспечения информационной безопасности (ИБ) и оценки текущего состояния ИБ ЦОСУ и СДО. Описана структурная схема концепции обеспечения ИБ ЦОСУ и СДО. Изложенный подход, на наш взгляд, способствует эффективной реализации комплексного взаимодействия как существующих, так и новых перспективных механизмов контроля и обработки информационных потоков, которые циркулируют в ЦОСУ и СДО.

Ключевые слова: информационная безопасность, университет, цифровая образовательная среда

Введение.

В постиндустриальном обществе непрерывное образование стало общим показателем тенденции повышения роли и значения постоянного обучения человека в соответствии с концепцией быстрого обновления знаний [1]. В то же время сегодня все шире проявляется возможность использовать самые передовые образовательные среды, платформы и новые учебные технологии в процессе обучения студентов в университетах. Информационные технологии (ИТ) уже давно стали неотъемлемой частью образования ведущих мировых лидеров – США, ЕС, Китая и др. государств. Современное дистанционное обучение (ДО) с использованием интернет-технологий и популярных web-сервисов стало формой получения образования, наряду с стационарной и заочной. Глобальные сети предоставляют огромные возможности для образования и самообразования. При этом в ДО используют лучшие педагогические методы и приемы, основанные как на традиционных, так и на инновационных средствах и формах обучения. Упор, однако, делается именно на широкое применение компьютерных и телекоммуникационных технологий.

Большинство специалистов в области ДО, рассматривают компьютерную технику и телекоммуникационные технологии как достаточно надежные системы. И рассчитывают с их помощью кардинально повысить качество обучения. Особенно это актуально для повышения результативности самостоятельной работы, а также при использовании внешнего контроля, выполняемых учащимися заданий. Однако, реализация подобной сложной задачи порождает достаточно большое количество проблем. Одной из них в современных условиях роста количества и сложности деструктивных вмешательств в работу информационных систем (ИС) цифровой образовательной среды, принятой в современных университетах (далее ЦОСУ), стала задача по обеспечению

информационной и кибербезопасности (ИБ и КБ) в системах ДО (или СДО). Задачи обеспечения ИБ в ЦОСУ и СДО, достаточно близки к аналогичным задачам, связанным с защитой в существующих системах обработки информации. Причем для многих подобных систем, например, в банках, и на промышленных предприятиях, уже наработана и успешно апробирована соответствующая законодательная и нормативная база. Также существуют и конкретные, хорошо зарекомендовавшие себя организационно-технические решения.

Методы и исследования.

Заметим, что как было показано в работах [2, 3], задачи по защите информации (ЗИ) в ЦОСУ в целом, и в СДО, имеют свою специфику. В частности, в качестве главных особенностей авторы [2, 3] указывают: территориально распределенные структуры СДО; разные платформы и не стандартизированное программное обеспечение для СДО; не стандартизированные технические решения для СДО; необходимость ЗИ, а также прав на интеллектуальную собственность, которая может одновременно принадлежать нескольким владельцам. В соответствии с [2], под ИБ ЦОСУ и СДО будем понимать состояние защищенности соответствующих интересов и ресурсов. Полагая, что для данных ресурсов и интересов существуют как внешние так внутренние угрозы.

Информационными ресурсами (ИР) в СДО являются: технические средства ДО (например, компьютеры, средства: связи, виртуализации учебного процесса и др.); электронные носители (вне зависимости от типа или вида); информация (файлы, базы данных, архивы, электронные библиотеки и др.).

Очевидно, что оценивать защищенность и надежность хранения информации в СДО удобно с помощью ряда интегральных показателей [1-3]. К таковым можно отнести: физическую целостность. То есть показатель, для оценивания отсутствия/наличия искажений информации в ЦОСУ и СДО; доверие к информации. Показатель, который позволяет оценивать отсутствие/наличие/подмену/несанкционированную модификацию информации; безопасность информации. То есть отсутствие/наличие возможности не санкционировано получить информацию лицами или процессами, у которых нет на это полномочий; невозможность несанкционированного тиражирования информации в СДО, если владелец не дает такого права.

Задачи решаемые в контексте обеспечения ИБ ЦОСУ и СДО должны быть направлены на то, чтобы: - выявить и прекратить попытки уничтожения/подмены, получения, несанкционированной модификации информации; ликвидировать последствия успешных реализаций киберугроз для СДО; выявить и нейтрализовать факторы, способствующие дестабилизации работы СДО, а также каналы утечки важной информации в СДО; выявить и нейтрализовать причины, повлекшие обнаружение дестабилизирующих факторов, в результате которых возникли утечки информации по выявленным каналам; определить лиц, которые своими действиями или бездействием привели к обнаружению дестабилизирующих факторов и/или формированию каналов утечки информации; др.

Таким образом, в результате проводимых мероприятий по обеспечению ИБ ЦОСУ и/или СДО должен быть предотвращен или сокращен ущерб (экономический, моральный, технический), который связан с фактами противоправного использования (повреждения/модификации) ИР.

Разработка защищённой ЦОСУ должно предваряться анализом рисков для подобных систем.

Задача анализа риска – это необходимый этап решения задач, связанных с задачей ЗИ. Этап проводят для того, чтобы выявить перечень возможных угроз ИБ ЦОСУ.

По результатам анализа рисков соответствующими структурами, ответственные за ИБ ЦОСУ лица, разрабатывают соответствующие политики безопасности (ПИБ). Данный документ (документы), как правило содержат перечень основных принципов организации ДО, основываясь на балансе образовательных задач и заданий по обеспечению ИБ ЦОСУ. Документ должен содержать перечень потенциальных угроз для ЦОСУ, определять требования к желаемому уровню защищенности тех или иных ИР, а также описывать организационно-технические решения, направленные на достижение заданного уровня защиты ЦОСУ.

Разработка ПИБ, также предполагает, анализ типовой или специфической для конкретного учебного заведения процесса организации и структуры ЦОСУ.

Так типовая структура ЦОСУ, принятая в современных университетах, предполагает наличие таких компонент: хранилище данных или репозиторий. Хранилище, служит для размещения необходимых в учебном процессе материалов (например, лекций, фильмов, аудиозаписей, презентаций и др.); ресурсы и инструменты для исследований (средства анализа данных, виртуальные лаборатории, обработка больших данных); облачные образовательные ресурсы и сервисы. К сервисам можно отнести стандартное или собственное программное обеспечения, средства тестирования и контроля и др. ресурсы и инструменты для поддержки и распространения научных исследований (электронная система поддержки конференций, электронные журналы, институциональные репозитории); цифровые научные сообщества: профиль исследователя, профиль университета (структурного подразделения); средства научной коммуникации; средства доступа к наукометрическим базам данных: публикация материалов, поиск научной информации; электронная библиотека университета; цифровые рейтинги университета; SMART технологии управления университетом.

Анализ структуры ЦОСУ и СДО университетов позволяет сконцентрировать внимание стороны защиты на наиболее узких в плане ИБ участках, а также оптимизировать затраты ресурсов, в частности финансовых, направленных на построение эффективных контуров защиты ЦОСУ.

В таких «узких» местах можно отнести: процедуры удаленной аутентификации студента; процедуры контроля доступа; процедуры обнаружения угроз для ЦОСУ и СДО; средства и методы защиты сетевых коммуникаций и информационно-коммуникационных технологий, используемых в ЦОСУ и СДО; средства и методы защиты репозитория.

Таким образом, существует явное противоречие между принципиальной возможностью разработки функционально устойчивых ЦОСУ и СДО на базе использования ИТ и недостаточной эффективностью существующих систем защиты информационных сетей университетов, которые не обеспечивают заданный уровень кибербезопасности и функциональной устойчивости СДО.

Основой создания методологии построения системы защиты информации (СЗИ) в ЦОСУ является структура "универсальная платформа - базовый подход к защите" ЦОСУ (рис. 1).

Для каждой из приведенных структур СЗИ в ЦОСУ, созданных по типовым технологиям, характерна своя многоуровневость в контексте выполнения функциональных задач.

Степень защищенности ЦОСУ обусловлена их архитектурой, функциональными особенностями, влиянием угроз, механизмами безопасности (ISO / IEC 15408).

Методологическим основанием построения СЗИ в ЦОСУ является создание базового подхода, одним из сегментов которого становится построение комплексных СЗИ на уровне "многоуровневая система управления ЦОСУ - многоуровневая защита" на основе парадигмы "объект - угроза - защита".

Согласно типовой архитектуры ЦОСУ базовый подход к построению СЗИ ЦОСУ направлен на решение таких задач - обеспечение конфиденциальности, целостности, доступности, наблюдаемости, гарантий в пространстве интеллектуализации учебного процесса и сохранения прав интеллектуальной собственности на инновационные разработки университета.



Рисунок 1 - Универсальная платформа - базовый подход к защите" ЦОСУ

Первоочередные меры по реализации политики ИБ (ПИБ) ЦОСУ должны быть направлены на разработку:

- стратегии защиты ИТ-инфраструктуры ЦОСУ;
- правил создания, обработки и хранения информации в ЦОСУ;
- правил по резервному копированию и восстановлению данных в ЦОСУ, в частности, для ликвидации последствий кибератак и др.

Базовый подход к ИБ ЦОСУ направлен на обеспечение конфиденциальности, целостности, доступности имеет иерархическую структуру, и основан на существующих стандартах в области ИБ, что предполагает реализацию следующих обязательных таких мероприятий:

Организационных:

- Создание ПИБ ЦОСУ и контроль ее выполнения;
- Введение правил использования учетных записей в ЦОСУ;
- Регулярные тренинги всех пользователей ЦОСУ по основам ИБ;
- Повышение квалификации ИТ-специалистов и администраторов ЦОСУ в области современных киберугроз и методов защиты;
- Проведение тестовых (учебных) атак;
- Тестирование уровня знаний сотрудников и пользователей о правилах ИБ;
- и т.д.

Технических:

- Мониторинг безопасности сети;
- Настройка сегментации сети;

- Обновление системного и прикладного программного обеспечения (ПО);
- Отказ от применяя сетевых дисков для хранения важной информации;
- Актуальное антивирусное ПО;
- Контроль запуска приложений и программ, используемых в ЦОСУ;
- Контроль подключения периферийных устройств и съемных носителей;
- и т.д.

Дополнительных, направленных на использование систем и инструментария:

- "Песочниц";
- контроля действий привилегированных пользователей;
- мониторинга и профилирования сетевых потоков;
- детектирования элементов ЦОСУ с целью превентивного обнаружения известных и новых уязвимостей;
- по централизованному сбору и анализу событий ИБ;
- сбора журнальной информации от СЗИ;
- и др.

Система ИБ ЦОСУ также основана на: модели угроз; модели нарушителя.

Мероприятия по внедрению контроля угроз на периметре ЦОСУ, будет включать использование:

- сетевых экранов;
- веб-шлюза безопасности;
- почтового шлюза безопасности;
- инструментария контроля доступа;
- средства и инструментарий для сегментации локальной сети университета и кампуса;
- средств изоляции портов;
- средств противодействия кибератакам;
- средств по блокировке прямого сетевого взаимодействия между корпоративным сегментом и непосредственно ЦОСУ;
- средств по контролю запуска приложений и ПО;
- средств для быстрой проверки ИБ ЦОСУ по заданным индикаторам.

Технология проектирования СЗИ для ЦОСУ осуществляется согласно задачам обеспечения безопасности - конфиденциальности, целостности, доступности, наблюдаемости, и их взаимосвязи в соответствии с ISO / IEC 15408.

На основе анализа моделей, предложенных в работах [4–11] сформируем методологические принципы построения системы обеспечения ИБ и оценки текущего состояния ИБ ЦОСУ и СДО, которые приведены на рис. 2. Опираясь на известный подход к построению методологий [4–11] и схему информационных потоков СДО с учетом необходимости обеспечения их кибербезопасности, предлагается принципиально новая методология построения системы обеспечения ИБ ЦОСУ и СДО. Методология содержит следующие этапы:

- 1) определение вероятности воздействия угроз ИБ на ЦОСУ и/или СДО;
- 2) определение обобщенного показателя уровня ИБ ЦОСУ и/или СДО;
- 3) оценки эффективности инвестиций в ИБ ЦОСУ и/или СДО;
- 4) построение интегрированных механизмов обеспечения ИБ ЦОСУ и/или СДО.

Предлагаемая структурная схема концепции обеспечения ИБ ЦОСУ и СДО, на наш взгляд, способна эффективно реализовать комплексное взаимодействие как существующих, так и новых перспективных механизмов контроля и обработки ИП, которые циркулируют в ЦОСУ и СДО.

Благодарности. Исследование финансируется Казахским национальным педагогическим университетом имени Абая (договор № ППС-ДН-01 от 12.02.2020)

СТРУКТУРНАЯ СХЕМА КОНЦЕПЦИИ ОБЕСПЕЧЕНИЯ ИБ И КБ СДО

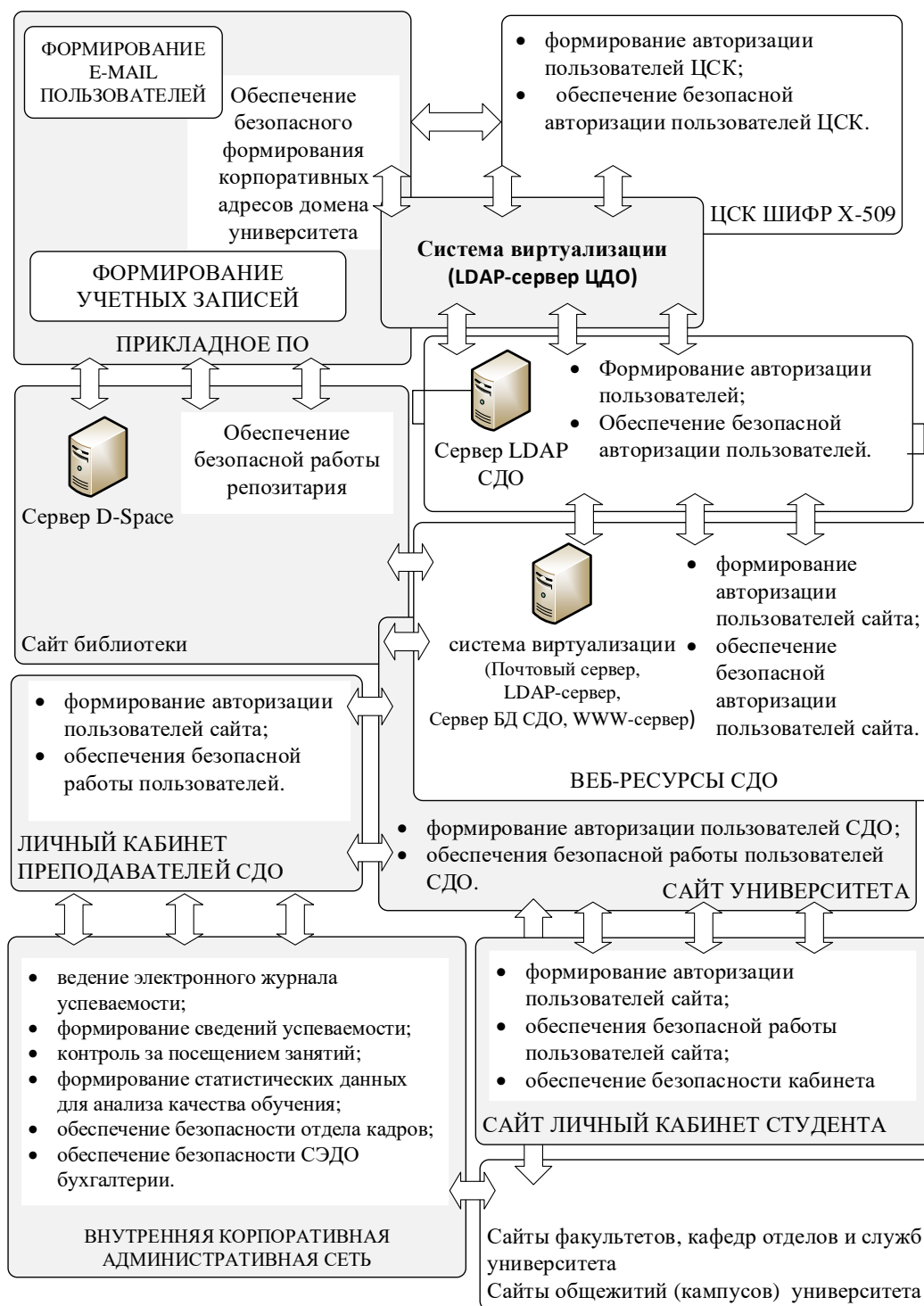


Рисунок 2 – Структурная схема Концепции обеспечения ИБ ЦОСУ и СДО

Выводы.

Концептуально изложены методологические принципы построения системы

обеспечения ИБ и оценки текущего состояния ИБ ЦОСУ и СДО. Описана структурная схема концепции обеспечения ИБ ЦОСУ и СДО. Изложенный подход, на наш взгляд, способствует эффективной реализации комплексного взаимодействия как существующих, так и новых перспективных механизмов контроля и обработки информационных потоков, которые циркулируют в ЦОСУ и СДО.

ЛИТЕРАТУРА

[1] Балыкбаев Т.О., Бидайбеков Е.Ы., Ахметов Б.С., Гриншкун В.В. Концепция цифровизации Казахского национального педагогического университета имени Абая. Алматы: КазНПУ имени Абая. Издательство «Ұлағат», 2020. – 122с.

[2] Ахметов Б.С., Ехлаков Ю.П., Силич М.П., Яворский В.В. Методология моделирования информационной образовательной среды вуза. Монография. – Алматы, 2008. – 275 с.

[3] Schneider, F.V.: Cybersecurity education in universities. IEEE Secur. Priv. 11(4), 3–4 (2013).

[4] Проталинский, Олег Мирославович, and Искандар Маратович Ажмухамедов. "Информационная безопасность вуза." Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика 1 (2009): 18–23.

[5] Долженко, Алексей Иванович, and Леонид Игоревич Потапов. "Анализ информационной безопасности образовательного процесса университета на базе нечетких моделей." Мягкие измерения и вычисления 30.5 (2020): 32–40.

[6] Lane, Tim. Information security management in Australian Universities: An exploratory analysis. Diss. Queensland University of Technology, 2007. P. 269.

[7] Schuett, Maria, and M. Rahman. "Information Security Synthesis in Online Universities." arXiv preprint arXiv:1111.1771 (2011).

[8] Singh, Vikas, and Madhusudhan Margam. "Information Security Measures of Libraries of Central Universities of Delhi: A Study." DESIDOC Journal of Library & Information Technology 38.2 (2018). p. 102–109.

[9] Akhmetov, B., Lakhno, V., Gusev, B., Lakhno, M., Porokhnia, I., Zhilkishbayeva, G., Akhanova, M. Adaptive Decision Support System for Scaling University Cloud Applications, (2021) Studies in Systems, Decision and Control, 337, pp. 49–60.

[10] Lakhno, V.A., Kasatkin, D.Y., Blozva, A.I., Gusev, B.S. Method and Model of Analysis of Possible Threats in User Authentication in Electronic Information Educational Environment of the University, (2020) Advances in Intelligent Systems and Computing, 938, pp. 600–609.

Ахметов Бахытжан Сражатдинович, т.ғ.д., Абай атындағы Қазақ ұлттық педагогикалық университетінің профессоры, Логистика және көлік академиясының профессоры, Алматы, Қазақстан, b.akhmetov@alt.edu.kz

Лакно Валерий Анатольевич т.ғ.д., Ұлттық биоресурстар және табиғатты пайдалану университетінің профессоры, Киев, Украина, lva964@gmail.com

АҚПАРАТТЫ ҚОРҒАУ ЖӘНЕ УНИВЕРСИТЕТТИҢ ЦИФРЛЫҚ БІЛІМ БЕРУ ОРТАСЫНЫҢ КИБЕРҚАУІПСІЗДІГІ

Аңдатпа. Қазіргі заманғы университеттің кибернетикалық қорғау тұрғысынан қауіпсіз болатын цифрлық білім беру ортасын (УЦББО) және оның қашықтықтан оқыту жүйесін (ҚОЖ) құру ерекшеліктері талданды. "УЦББО қорғаудың базалық тәсілінің" әмбебап платформасы сипатталған. Ақпараттық қауіпсіздікті (АҚ) қамтамасыз ету жүйесін құрудың және ҚОЖ және УЦББО АҚ ағымдағы жай-күйін бағалаудың әдіснамалық қағидаттары тұжырымдамалық түрде баяндалған. ҚОЖ және УЦББО АҚ қамтамасыз ету тұжырымдамасының құрылымдық схемасы сипатталған. Жоғарыда аталған тәсіл, біздің ойымызша, УЦББО мен ҚОЖ-да айналатын ақпараттық ағындарды бақылау мен өңдеудің қолданыстағы және жаңа перспективалық тетіктерінің кешенді өзара іс-қимылын тиімді іске асыруға ықпал етеді.

Түйінді сөздер: ақпараттық қауіпсіздік, университет, цифрлық білім беру ортасы.

Akhmetov Bakhytzhan Srazhatdinovich, doctor of technical sciences, professor of the Abai Kazakh National Pedagogical University, professor of the Academy of logistics and transport, Almaty, Kazakhstan, b.akhmetov@alt.edu.kz

Lakhno Valery Anatolyevich, doctor of technical sciences, professor of the National University of Bioresources and nature management, Kiev, Ukraine, lva964@gmail.com

INFORMATION PROTECTION AND CYBERSECURITY OF THE UNIVERSITY'S DIGITAL EDUCATIONAL ENVIRONMENT

Abstract. The features of building a cybernetic-safe digital educational environment of a modern university (DEEMU) and its distance learning system (DLS) are analyzed. The universal platform "Basic approach to DEEMU protection" are described. Conceptually, the methodological principles of building an information security system (IS) and assessing the current state of the IS of the DEEMU and DLS are outlined. The structural scheme of the concept of providing IS of DEEMU and DLS are described. The described approach, in our opinion, contributes to the effective implementation of complex interaction of both existing and new promising mechanisms for monitoring and processing information flows that circulate in the DEEMU and DLS.

Keywords: information security, university, digital educational environment.
