Scientific and Practical Cyber Security Journal (SPCSJ) 5(3): 25-29 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

О НЕОБХОДИМОСТИ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ И ТЕХНОЛОГИЯХ
ON THE NEED TO ENSURE CYBERSECURITY IN EDUCATIONAL INFORMATION SYSTEMS AND TECHNOLOGIES

д.т.н., профессор Хлапонин Юрий Иванович,Киевский национальной университет строительства и архитектуры, г. Киев, Украина
Doctor of Technical Sciences, Professor Yuri Khlaponin,Kiev National University of Civil Engineering and Architecture, Kiev, Ukraine
к.т.н., Козубцова Леся Михайловна, Военный институт телекоммуникаций и информатизации имени Героев Крут, г. Киев, Украина
Ph.D., Lesya Kozbtsova,Military institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine
д.п.н., профессор РАЕ Козубцов Игорь Николаевич, Научный центр связи и информатизации Военного института телекоммуникаций и информатизации, г. Киев, Украина
Doctor of Pedagogical Sciences, Professor of RAE, Igor Kozubtsov,Scientific center of communication and Informatization of the Military Institute of telecommunications and Informatization, Kiev, Ukraine

АННОТАЦИЯ. Актуальность темы исследований о необходимости обеспечения кибербезопасности информационных систем и технологий в образовании обусловлена постоянно возрастающей уязвимостью, а также скрытым рыском потери активов учебных заведений.

Основных аспекты работы. В статье поднимается вопрос о необходимости рассмотрения обеспечения кибербезопасности информационных систем и технологий в образовании. Установлено, что в данное время исследователями не приделано надлежащего внимания вопросу обеспечения кибербезопасности в проектируемых информационных системах и технологиях в сфере образования.

Научная новизна. Научная новизна темы заключается в постановке задании о необходимости решение научно-практической задачи обеспечения кибербезопасности информационных систем и технологий в образовании.

КЛЮЧЕВЫЕ СЛОВА: *кибербезопасность, образование, информационная система, технология, деструктивное информационное влияние, киберзащищенность, методика.*

ABSTRACT. The relevance of the research topic on the need to ensure the cybersecurity of information systems and technologies in education is due to the constantly increasing vulnerability, as well as the hidden risk of losing assets of educational institutions.

The main aspects of the work. The article raises the question of the need to consider the provision of cybersecurity of information systems and technologies in education. It is established that at this time, researchers have not paid proper attention to the issue of ensuring cybersecurity in the projected information systems and technologies in the field of education.

Scientific novelty. The scientific novelty of the topic lies in the formulation of a task about the need to solve the scientific and practical problem of ensuring the cybersecurity of information systems and technologies in education.

KEYWORDS: *cybersecurity, education, information system, technology, destructive information influence, cyber security, methodology.*

ВВЕДЕНИЕ. В настоящее время наблюдается высокий интерес исследований, который отображен в диссертационных работах ученых по направлению разработки моделей и информационных технологий обеспечения гармонизации высшего образования. Анализируя одну из таких работ, например, [1] на удивление нами не было выявлен актуального аспекта, а именно, каким образом обеспечивается кибербезопасность указанной информационной системы. В связи с этим возникают два очевидных вопроса:

1) почему проектанты информационных системы пренебрегают кибербезопасностью?

2) осознают ли проектанты информационных системы катастрофической опасности в результате нарушения кибербезопасности?

Поэтому, учитывая выше изложенного, по нашему мнению, возникла необходимость в данной работе рассмотреть отдельные аспекты, которые связанны с необходимостью обеспечение кибербезопасности в

информационных системах и технологиях, что предлагаются в образовании.

АНАЛИЗ ПОСЛЕДНИХ ИССЛЕДОВАНИЙ И ПУБЛИКАЦИЙ ПО ДАННОМУ НАПРАВЛЕНИЮ

Автор работы [2] приводит перечень проблем, возникающих при использовании информационных технологий в образовательном контексте. Также он даёт характеристику потенциальным угрозам кибербезопасности: несанкционированный доступ к данным, фильтрация нежелательной информации, кибертерроризм. Но к сожалению, не рассматривается такой важный и актуальный аспект, как кибербезопасность информационной технологий в образовании. Но в отличии от этой работы в статье [3] затрагивается проблема обеспечения кибербезопасности систем дистанционного обучения образовательных учреждений. Результатом работы стало известно об наличии основных факторов риска безопасности, а также виды и источники угроз систем дистанционного обучения образовательных учреждений. Полученные новые знания подводят на мысль о необходимости обеспечения кибербезопасности в образовательных информационных системах и технологиях, объектом исследования которая выступают в данном исследовании.

ЦЕЛЬ СТАТЬИ

Рассмотрение вопроса о необходимости обеспечение кибербезопасности в существующих и проектируемых информационных систем и технологиях в образовании.

ОСНОВНОЙ РЕЗУЛЬТАТ ИССЛЕДОВАНИЯ

Для понимания вопроса о необходимости решения проблемы обеспечения кибербезопасности информационных систем и технологий в образовании, обусловлено рассмотрение сущности с методологической точки зрения толкование дефиниции “информационных систем” и “информационной технологии”. Затем изучить источники возможных киберугроз, а также возможные уязвимости информационных систем и технологий в образовании.

Поскольку дефиницию “информационных систем” ми подробно рассматривали в публикации [4], где сделаны соответствующие выводы, поэтому с точки зрения понимания уязвимости к киберугрозам будут интересны следующие два определения:

согласно ДСТУ 2392-94 [5] «информационная система» – это коммуникационная система, обеспечивает сбор, поиск, обработку и пересылку информации;

ISO/IEC 2382:2015 [6] «информационная система» – система, предназначенная для сбора, хранения, обработки, передачи и использования информации”.

Исходя из этих определений резюмируя понятия «информационная система» – это совокупность технических, вычислительных средств, которые обеспечивают сбор, поиск, обработку и пересылку информации. Как показывает современная практика они в большей степени подвержены киберугрозам.

Целесообразная необходимость обеспечения киберзащищенности информационных систем и технологий основывается на следующих постулатах:

1. Не существует абсолютной киберзащищенности систем управления.
2. Чем более сложная система, чем больше задач она выполняет, тем ниже ее киберзащищенность.
3. Необходимым условием повышения киберзащищенности системы является введение избыточности в сочетании с организацией эффективного контроля.
4. Киберзащищенность системы управления должна обеспечиваться на всех этапах жизненного цикла.
5. Уровень киберзащищенности системы ограничен экономическими рисками заказчика и эксплуатирующей организации.

Таким образом, абсолютной киберзащищенности невозможно достичь, поскольку устранение одних уязвимостей в системе не исключает возможности появления новых, что свидетельствует современная практика.

Целью применения деструктивных информационных влияний (кибератаки) на информационную систему является нарушение одного или комплекса перечислений, а именно: конфиденциальности и целостности информации, доступности информационной системы или содержащихся в ней данных (рис. 1).

С учетом этого, категорию кибербезопасности информации, которая циркулирует в информационной системе образования $K_{КБ}(S)$, можно представит следующим выражением (1):

(1)

где K – конфиденциальность;

Ц – целостность;

Д – доступность.

Учитывая выражение (1) кибербезопасность системы $K_{КБ}(S)$ можно представить через потерю конфиденциальности, целостности или доступности данных [7, с. 36] (2):

$$K_{КБ}(S) = 1 - (1 - P_{К_i})(1 - P_{Ц_i})(1 - P_{Д_i}) \quad (2)$$

где $P_К$, $P_Ц$, $P_Д$ – соответствующие вероятности нарушения конфиденциальности, цельности и доступности

информации в информационной системе образования.

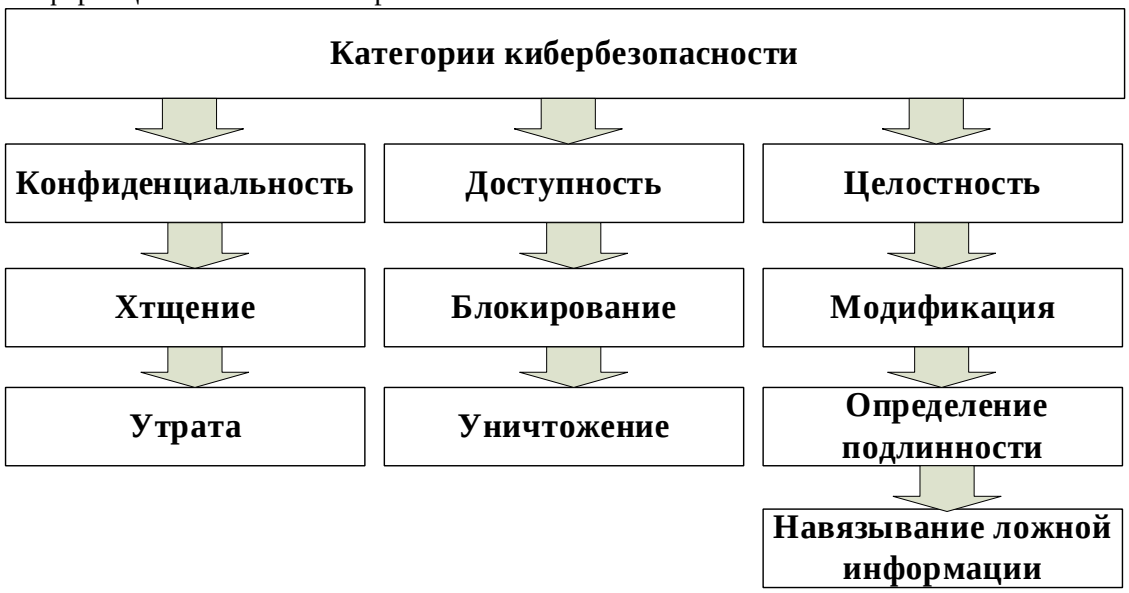

Рис. 1 Категории кибербезопасности

Нарушения кибербезопасности, то есть потери конфиденциальности, целостности или доступности, подробно рассматривается в работе [8, с. 110 – 112] через механизм способов их реализации. Поэтому нет смыла повторного рассмотрения.

Перейдем к рассмотрению дефиниции “информационной технологии”. Информационная технология – это совокупность методов, производственных процессов, программно-технических и лингвистических средств, интегрируемых с целью сбора, обработки, хранения, распространения, отображения и использования информации в интересах ее пользователей. [9, с. 61]. Более в упрощённом случая информационная технология – это совокупность методов, средств, приемов, обеспечивают поиск, сбор, хранение, обработки, представления, передачи информации между людьми. Как видим, в основу информационной системы закладывается информационная технология. Другими словами, функционирование информационной системы, которая обеспечивает сбор, поиск, обработку и пересылку информации осуществляется по разработанной информационной технологии, которая и определяет какие именно применять методы, средства, приемы, обеспечивают поиск, сбор, хранение, обработки, представления, передачи информации. Исходя из этого и свидетельства современной практики информационные системы уязвимы к деструктивным информационным воздействиям (кибервлияниям).

Рассмотрим режимы работы информационных систем: автономный (закрытый); общедоступный (открытый). Исходя из режимов работы информационных систем вытекают возможны варианты кибервлияний (табл. 1).

Таблица 1 – Возможные варианты кибервлияния с учетом режимов работы информационных систем

№ п/п	Источники кибервлияния	режимы работы системы	
		автономный	открытый (общедоступный)
1	внутренние	+	+
2	внешние	–	+

Если мы рассматриваем закрытую от внешнего мира информационную систему, то источником нарушения кибербезопасности, как правило, является только человек-инсайдер этой системы, поскольку влияний с внешней не будет.

В отрытом режиме использования информационная система в образовании к существующим внутренним источникам кибервлияниям могут присоединяться и внешние. Источником внешних кибервоздействий на образовательную систему может стать кто-либо угодно имеющий достаточный опыт в применении средств кибервлияний и соответствующую мотивацию.

Рассмотрим классификацию нарушений кибербезопасности связанной с человеческим фактором, которую представлено в табл. 2.

При комбинированном случае источниками являются нарушители выше рассмотренных случаев.

Учитывая данные критерии (конфиденциальность, цельность и доступность) необходимо осуществить декомпозицию информационной системе образования S, то есть разложить ее на составляющие – средства и компоненты, которые уязвимы к воздействию деструктивным информационным воздействиям.

После этого, необходимо осуществить мониторинг киберзащищенности компонентов информационной системе образования на предмет их уязвимости. Для этого достаточно воспользоваться ранее предложенным методом мониторинга киберзащищенности информационной системы, предложенный в работе [10].

Таблица 2 – Классификация нарушений кибербезопасности связанной с человеческим фактором

№ п/п	Человеческий фактор	Уровень пользователей системы	
		Пользователь (обучаемый)	Администратор (обучающий)
1	недовольные сотрудники	+	+
2	шпионаж	+	+
3	халатность	+	+
4	низкая квалификация	+	+
5	шантаж	+	+

По его итоге киберзащищенности информационной системы необходимо оценить уровень защищенности и за необходимости осуществить соответствующую корректировку киберзащищенности.

Технические сбой мы опускаем с рассмотрение, поскольку он больше связан с технической надежностью технических средств, реализовывает информационную систему. Практика показывает, что уже через 5 лет эксплуатации компьютеров, в следствие морального старения, целесообразно заменять их на новые, хотя физическое старения или износ их далекие от предельного состояния. Это связано с тем, что кривая морального старения объекта пересекает и превышает предельно допустимый уровень показателя цена/качество и, следовательно, дальнейшая его эксплуатация нерентабельна [11].

О грядущей проблеме кибербезопасности в образовательных информационных системах и технологиях всеобщая идеология максимального внедрения дистанционных форм обучения. В данном случай используется только общедоступный режимы работы информационной системы дистанционного обучения транспортной системой которой выступает Интернет. Прошло то время, когда обучение происходило посредством выполнения домашних контрольных заданий с последующей их отправкой по почте.

Рассмотрим наиболее уязвимые сточки зрения кибербезопасности части информационной технологии. Для этого представим процесс, который протекает в информационной технологии в виде этапов следующего алгоритма:

этап 1 поиск информации;
этап 2 сбор информации;
этап 3 хранение информации;
этап 4 обработка информации;
этап 5 представление информации;
этап 6 передачи информации.

Каждый этап процесса информационной технологии важен для правильности функциональной работы проектируемой информационной системы. Если нарушить доступность к информационной системе образования, то очевидно, что и нарушатся (приостановятся) протекающие в ней процессы информационной технологии.

ВЫВОДЫ

Таким образом, строить полноценную комплексную систему защиты информации (КСЗИ) в проектируемых информационных системах образования возможно не стоит, но необходимо соблюдать (обеспечивать) превентивную кибербезопасность (кибергигиену) не только когда она соприкасается с внешним киберпространством, но, когда находится в автономном режиме.

Для понимания взаимосвязей очень удобно пользоваться моделью основных понятий безопасности и характер связей между ними разработанный в DUS ISO/IEC 27032: 2012 [12]. Эта модель позволяет наглядно представить для понимания взаимосвязи между кибербезопасностью и источниками угроз для дальнейшего моделирования мероприятий по предотвращению киберугроз.

Необходимо рекомендовать исследователям в предлагаемых ими информационных системах и технологиях описывать меры обеспечения кибербезопасности.

ПЕРСПЕКТИВЫ ДАЛЬНЕЙШИХ НАУЧНЫХ ИССЛЕДОВАНИЙ

Разработка методики планирования кибербезопасности информационных системах и технологиях в образовании.

СПИСОК ЛИТЕРАТУРЫ

1. Цюцюра М.І. Інформаційні технології гармонізації зрівноваженого освітнього простору: автореф. дис. ... д-ра техн. наук: 05.13.06; Київ. нац. ун-т буд-ва і архітектури. Київ, 2020. 44, с.
2. Зубалова О.А. Проблемы информационной безопасности образовательной среды в современныхусловиях // Мир науки, культуры, образования. 2018. № 3 (70). С. 36 – 38. ISSN 1991-5497.
3. Оладько В.С. Риски киберзопасности систем дистанционного обучения // Международный научно-исследовательский журнал. 2019. № 10 (88). С. 31 – 34.
4. Козубцова Л.М., Кіт Г.В., Ліщина В.О., Козубцов І.М. Аналіз змісту поняття інформаційна системи спеціального призначення // Materials of the XVI International scientific and practical Conference Cutting-edge science – 2020, April 30 – May 7, 2020 Construction and architecture. Mathematics. Modern information technology. Technical science: Sheffield. Science and education LTD, 2020. Volume 8. Pp. 56 – 58.
5. ДСТУ 2392-94 “Інформація та документація. Базові поняття”. К.: УкрНДІССІ, 1994. 25 с.
6. ГОСТ 33707-2016 (ISO/IEC 2382:2015) Информационные технологии (ИТ).
7. Тутубалин П.И., Моисеев В.С. Вероятностные модели обеспечения информационной безопасности автоматизированных систем обработки информации и управления: монография. Казань: РИЦ «Школа», 2008. 144 с. (Серия «Современная прикладная математика и информатика»).
8. Дроботун Е.Б. Теоретические основы построения систем защиты от компьютерных атак для автоматизированных систем управления. Монография. СПб.: Наукоемкие технологии, 2017. 120 с.
9. Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. – М.: Институт развития информационного общества, 2009. 160 с.
10. Козубцова Л.М. Удосконалена методика діагностування кібернетичної захищеності інформаційної системи з урахуванням деструктивних кібернетичних впливів. Науковий журнал «Комп'ютерно-інтегровані технології: освіта, наука, виробництво». Луцьк, 2020. Випуск № 39. С. 127 – 135.
11. Шубинский И.Б. Структурная надежность информационных систем. Методы анализа. М.: «Журнал Надежность», 2012. 216 с.
12. DUS ISO/IEC 27032: 2012. Information technology – Security techniques – Guidelines for cybersecurity. 61 p.