CZU: 378:004.056.5 DOI: 10.36120/2587-3636.v32i2.20-26

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ВЫСШЕГО ОБРАЗОВАНИЯ С ПЕРСПЕКТИВЫ КЛАССИФИКАЦИИ ИНФОРМАЦИОННЫХ АКТИВОВ

Любомир КИРИЯК, доктор физико-математических наук, профессор
https://orcid.org/0000-0002-5786-5828
Виолетта БОГДАНОВА, кандидат педагогических наук
https://orcid.org/0000-0003-4140-6317
Анна СВИНАРЕВА, доктор экономических наук, доцент
https://orcid.org/0000-0002-8598-3717
Одесский Национальный Политехнический Университет, Украина

Аннотация. В статье рассмотрены угрозы, возникающие в информационной среде высшего учебного заведения. Оценены риски возникновения угроз нарушения целостности, конфиденциальности и доступности. В соответствии с представленными категориями информационных активов высшего учебного заведения описаны необходимые мероприятия по их защите.

Ключевые слова: информационная безопасность, политика обеспечения информационной безопасности в вузе, информационные активы, информационные угрозы, средства защиты.

ENSURING INFORMATION SECURITY IN THE HIGHER EDUCATION SYSTEM FROM THE PERSPECTIVE OF CLASSIFYING INFORMATION ASSETS

Liubomir CHIRIAC, hab. doctor of physical and mathematical sciences, professor
Violeta BOGDANOVA, PhD in education
Hanna SVINAROVA, doctor of economic sciences, assistant professor
Odessa Polytechnic National University, Ukraine

Abstract. The article considers the threats arising in the information environment of a higher educational institution. The risks of threats to integrity, confidentiality and accessibility are assessed. In accordance with the presented categories of information assets of the higher educational institution, the necessary measures for their protection are described.

Keywords: information security, information security policy at the university, Information assets, information threats, means of protection

1. Введение

В современных условиях постоянно увеличиваются угрозы информационной безопасности на всех уровнях: государства, организаций и личности. Обеспечение информационной безопасности играет важнейшую роль в обеспечении национальной, региональной и международной безопасности. Безопасность информационной сферы нельзя воспринимать только как защиту телекоммуникационных сетей от проникновения нежелательной или вредной информации без учета антропогенной составляющей, включающей в себя

значимую совокупность проблем, связанных с соблюдением конституционных прав и свобод граждан в сфере духовного развития и информационной деятельности.

Для системы высшего образования риски, связанные с кибератаками, выходят за рамки только финансовых потерь. В образовательных учреждениях хранится огромный объем конфиденциальных данных, от персональной информации студентов до ценной интеллектуальной собственности, которая в случае кражи или компрометации может нанести значительный ущерб далеко за пределами вуза. Кибератаки представляют собой серьезную угрозу для репутации вуза и безопасности его студентов, возможно, даже более значительную, чем потенциальные финансовые потери.

Цель исследования состоит в формулировании требований к организации системы информационной безопасности в высшем учебном заведении с позиции категорирования информационных активов.

Задачи исследования: проанализировать особенности информационной среды высшего учебного заведения, определить возникающие информационные риски, рассмотреть способы защиты информации с позиции категорирования информационных активов.

Объект исследования – информационная безопасность высшего учебного заведения. *Предмет исследования* – содержание политики информационной безопасности высшего учебного заведения с позиции категорий информационных активов.

Методы исследования – индукция и дедукция, изучение и анализ научной литературы, международных стандартов, международного опыта, наблюдение, системный подход.

Степень изученности темы. В Республике Молдова вопросам информационной безопасности значительное внимание уделяется в работах Охрименко С., Cojocaru I., Zgureanu A. Bădărău E., Guzun, M., Rotari A., Bragaru T., Briceag V., Popov L., Скринпник Н. и др. Однако вопросы организации системы обеспечения информационной безопасности информации с позиции классификации информационных активов в высшем учебном заведении остаются недостаточно освещенными в научной литературе.

2. Специфика информационной среды высшего учебного заведения

В современном вузе хранится и обрабатывается огромное количество различных данных, связанных не только с обеспечением учебного процесса, но и с научно-исследовательскими и проектно-конструкторскими разработками,

персональные данные студентов и сотрудников, служебная, коммерческая и иная конфиденциальная информация [1].

Информационная среда высшего учебного заведения определяется совокупностью:

- субъектов информационных процессов;
- информационной инфраструктуры;
- информационного пространства;
- информационных ресурсов;
- общественных отношений, связанных с формированием, хранением, передачей и распространением информация.

Постоянно увеличивающийся рост количества преступлений в области информационной безопасности выдвигает новые требования к защите информационных ресурсов и информационных систем учебных заведений.

Система информационной безопасности включает в себя набор формальных и неформальных средств защиты: физических, программных, технических, правовых, организационных, морально-этических. Построение системы информационной безопасности осуществляется посредством формирования концепции безопасности образовательного учреждения, разработку регламентирующих документов, содержащих элементы нормативно-правового характера и организационных процедур по формированию безопасной среды вуза. Все это определяет единую политику обеспечения информационной безопасности в вузе.

Учитывая, что в высшем учебном заведении большинство обучающихся – это молодые люди в возрасте от 18 до 23 лет, обладающие достаточно высоким уровнем подготовки, энтузиазмом, максимализмом, то становится понятным их желание выделиться перед сокурсниками посредством получения административного доступа к локальной сети, заражения компьютеров вредоносным программным обеспечением, демонстрации превосходства над преподавателем и т.д. Необходимо также помнить, что высшие учебные заведения получили первыми доступ в сеть Интернет, а также именно в стенах университета были созданы первые вирусы. Таким образом, вуз зачастую становится местом повышенной активности «начинающих киберпреступников» [1, с.18].

Высшее учебное заведение также характеризуется многопрофильным характером деятельности, сложностью происходящих деловых процессов, необходимостью постоянного электронного взаимодействия с вышестоящими инстанциями, развитой инфраструктурой, наличием вспомогательных структур и филиалов, множеством форм и методов учебной работы, постоянной адаптацией к

меняющемуся рынку образовательных услуг, частым изменением статуса сотрудников и обучаемых.

3. Оценка риска информационных угроз в вузе

В соответствии с международными стандартами [3,4] процесс анализа рисков информационной безопасности состоит из идентификации рисков, установления их значений, а также процедуры оценки.

Каналы передачи информации в высшем учебном заведении включают в себя:

- процесс делопроизводства;
- сотрудничество с организациями, другими высшими учебными заведениями в стране и за рубежом;
- конференции, совещания;
- мероприятия в рамках приемных кампаний, привлечения абитуриентов, прочая профориентационная деятельность;
- научные исследования;
- инспекторат и надзорные органы.

Источниками конфиденциальной информации в высшем учебном заведении являются:

- персонал организации;
- носители информации (документы, флеш-накопители, изделия);
- технические средства хранения и обработки информации;
- средства коммуникации;
- сообщения.

В информационном пространстве вуза, включающего в себя разные автоматизированные информационные подсистемы (бухгалтерия, библиотека, деканат, кадры и т.д.) возможна реализация внутренних и внешних угроз по нарушению целостности, конфиденциальности и доступности информации:

- попытки несанкционированного доступа к базам данных;
- незаконный аудит сети вуза или других организаций;
- удаление информации, в том числе библиотек;
- запуск игровых программ;
- установка вредоносного программного обеспечения;
- установка нелицензионного программного обеспечения;
- поиск уязвимостей в операционных системах, межсетевых экранах, серверах и т. п.

В процессе оценки риска устанавливается ценность информационных активов, выявляются потенциальные угрозы и уязвимости, ранжирование приоритетов.

4. Информационные активы вуза и мероприятия по защите

При построении системы организационной защиты информации в высшем учебном заведении целесообразно руководствоваться следующими принципами:

1) *принцип комплексного подхода* – эффективное использование сил, средств, способов и методов защиты информации;
2) *принцип оперативности принятия управленческих решений* –нацеленность руководства и персонала на решение задач защиты информации;
3) *принцип персональной ответственности* – распределение задач по защите информации между руководством и персоналом и определение ответственности за полноту и качество их выполнения.

Категорирование информационных активов по степени их критичности осуществляется подразделением – владельцем информационного актива с учетом свойств: доступности, целостности и конфиденциальности. Для каждой категории информации определяются типовые требования информационной безопасности и принимается комплекс защитных мер.

Принципы категорирования объектов информационной инфраструктуры, определяющие взаимозависимость между категориями информационных активов, оборудования, на котором эта информация обрабатывается и (или) хранится, помещений, в которых размещено оборудование и комплекса предлагаемых защитных мер, снижающих риски несанкционированного доступа к информационным активам, представлены в таблице.

Таблица. Категорирование информационных активов по степени их критичности

Категория	Тип ИА	Реализация угрозы	Регламентация	Защитные меры
ИА0	государственная тайна	ущерб государственной безопасности	нормативные документы в области защиты государственной тайны	свои регламенты и правила
ИАI	ноу-хау, научные исследования, платежные документы	прямой (невосполнимый) ущерб	закон об авторском праве, о товарах, промышленных моделях и т.п.	специальные требования к оборудованию серверных помещений: система контроля управления доступом, видеонаблюдение, укрепленность дверей,

				оконных проемов, стен
ИАII	конфиденциальная информация	прямой ущерб	закон о коммерческой тайне, о служебных тайнах	требования к дополнительным мерам по настройке рабочих станциях и контролю доступа в помещения (система контроля управления доступом, кодовые замки)
ИАIII	служебная информация	опасен систематический несанкционированный доступ, разовый – не наносит ущерба	внутренние акты организации	стандартная парольная защита входа в систему на рабочих станциях
ИАIV	свободный доступ	отсутствует	отсутствует	не требуются защитные меры

Анализируя таблицу, можно видеть, что в высшем учебном заведении присутствуют практически все категории информационных активов. Соответственно, при оценке рисков реализации информационных угроз, необходимо классифицировать каждый актив и в соответствии с категорией принять соответствующие защитные меры.

5. Выводы

Внедрение средств управления информационной безопасностью жизненно важно для защиты информационных активов высшего учебного заведения, а также его репутации, студентов, персонала, других материальных или нематериальных активов.

Создание системы защиты информации с позиции категорирования информационных активов, регламентации соответствующих норм защиты, непрерывное повышение эффективности системы защиты информации, неукоснительное соблюдение персоналом установленных норм и правил защиты конфиденциальной информации, – все это будет способствовать повышению уровня информационной безопасности в высшем учебном заведении.

Благодарности. *Исследование поддержано проектом «Методология внедрения ИКТ в процесс изучения реальных дисциплин в системе образования Республики Молдова с точки зрения меж/трансдисциплинарности (концепция STEAM)», 20.80009.0807.20, включенный в «Государственную программу (2020-2023) Национального агентства развития и исследований.*

Библиография

1. ПРОТАЛИНСКИЙ, О. М.; АЖМУХАМЕДОВ, И. М. Информационная безопасность вуза. В: *Вестник АГТУ. Сер. Управление, вычислительная техника и информатика*, 2009. № 1 . ISSN 2072-9502. с. 18-23.
2. БЕЙДИНА, Т.Е.; КУХАРСКИЙ, А.Н. Политика информационной безопасности: критическое исследование содержания университетской политики. В: В*естник Забайкальского государственного университета*, 2021. т.27. № 4. с.55-72.
3. ISO/IEC 27005, Information technology — Security techniques — Information security risk management.
4. ISO/IEC 27001:2013, Information technology – Security Techniques – Code of practice for information security controls.
5. СИРОТЮК, В. О. Модели, методы и средства разработки и внедрения эффективной системы управления информационной безопасностью патентного ведомства. В: *Интернет-журнал «Науковедение»,* 2017. том 9, №6. https://naukovedenie.ru/PDF/06TVN617.pdf.