Т. 10. №3. 2024
https://doi.org/10.33619/2414-2948/100

УДК 372.862: 004.056.5 https://doi.org/10.33619/2414-2948/100/67

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ПОТОКОВ КАФЕДРЫ В ВУЗЕ

©Дозморов К. М., *ORCID: 0009-0008-3419-1104, SPIN-код: 6880-6747, Казанский национальный исследовательский технологический университет, г. Нижнекамск, Россия, dozmorovkirill@gmail.com*
©Яковлева Е. В., *ORCID: 0000-0002-1743-8645, SPIN-код: 6836-4135, д-р пед. наук, Казанский национальный исследовательский технологический университет, г. Нижнекамск, Россия, YakovlevaEV@inbox.ru*

ENSURING THE SECURITY OF INFORMATION FLOWS AT UNIVERSITY DEPARTMENTS

©Dozmorov K., *ORCID: 0009-0008-3419-1104, SPIN-code: 6880-6747, Kazan National Research Technological University, Nizhnekamsk, Russia, dozmorovkirill@gmail.com*
©Yakovleva E., *ORCID: 0000-0002-1743-8645, SPIN-code: 6836-4135, Dr. habil., Kazan National Research Technological University, Nizhnekamsk, Russia, YakovlevaEV@inbox.ru*

Аннотация. Актуальность исследования обусловлена тем, что на основе проведенного аудита вузовской кафедры раскрываются возможные угрозы информационной безопасности ее информационных потоков. Целью нашего исследования явилось выявление информационных потоков кафедры и комплексный анализ эффективных способов их защиты. Объект исследования — процесс обеспечения безопасности информационных потоков кафедры в вузе. Предмет исследования — создание схемы информационных потоков кафедры и схемы сетевого взаимодействия кафедры в вузе на основе политики доступа пользователей. Особое внимание в статье уделяется описанию выявленных потенциальных рисков, возникающих в результате несанкционированного доступа, внешних или внутренних атак. Важно отметить, что представленные направления работы по улучшению безопасности информационных потоков кафедры в вузе, являются приложением существующих общих способов защиты информации, необходимых для практического использования в учебном процессе. Показана возможность осуществления безопасности прикладного программного и сетевого обеспечения кафедры.

Abstract. The relevance of the study is caused by possible threats to the information security of information flows at the university department revealed during the latest information security audit. The purpose of our research is to detect information flows of the department and a detailed analysis of methods for their protection. The object of the study is the process of ensuring security of information flows at the university department. The subject of the research is the creation of information flow schemes of the department and developing network interaction schemes of the university department based on the user access policy. Particular attention is paid to the description of the identified potential risks arising from unauthorized access, external or internal attacks. It is important to note that the suggested ideas to improve the security of information flows of the university department are an application of existing methods of protecting information necessary for practical use in the educational process. The possibility of implementing the security of applied software and network support of the department is shown.

Т. 10. №3. 2024
https://doi.org/10.33619/2414-2948/100

Ключевые слова: информационная безопасность, информационные потоки, аудит информационной безопасности.

Keywords: information security, information flows, information security audit.

В Казанском национальном исследовательском технологическом университете на кафедре информационных систем и технологий (кафедра ИСТ) занимается изучением и разработкой информационных систем, применением технологий в области информационных технологий. Кафедра предоставляет студентам доступ к базам данных и библиотечным фондам, а также наглядные пособия, аудио-, видео- и мультимедийные материалы по всем вузовским дисциплинам и видам занятий. Аль-Хаммуд Ибрахим справедливо отмечает, что в любой сфере обработки данных, остро стоит проблема защиты информации [1]. В связи с этим аудит информационной безопасности кафедры является неотъемлемой частью общей стратегии обеспечения безопасности и защиты информации, способствующей улучшению защиты информационных активов. К основным информационным потокам кафедры ИСТ в нашем вузе (Рисунок 1) относятся:

1) Потоки учебной информации, которые передаются студентам и преподавателям через электронные платформы, электронную почту или внутренние информационные системы, включающие информацию о расписании занятий, учебных материалах, заданиях, оценках и другие данные, связанных с учебным процессом.

2) Потоки научной информации, передающиеся через доступ к научным библиотекам, журналам, материалам конференций и семинаров, а также через внутренние базы данных.

3) Потоки административной информации, передающиеся через официальную корреспонденцию, внутренние системы управления или встречи. Они включают информацию о персонале, бюджете, организационных процессах, совещаниях и других административных вопросах.

4) Потоки коммуникации с внешними партнерами, клиентами и другими заинтересованными сторонами. Они могут включать запросы на сотрудничество, договоры, отчеты о выполнении проектов и другие коммерческие и деловые данные.

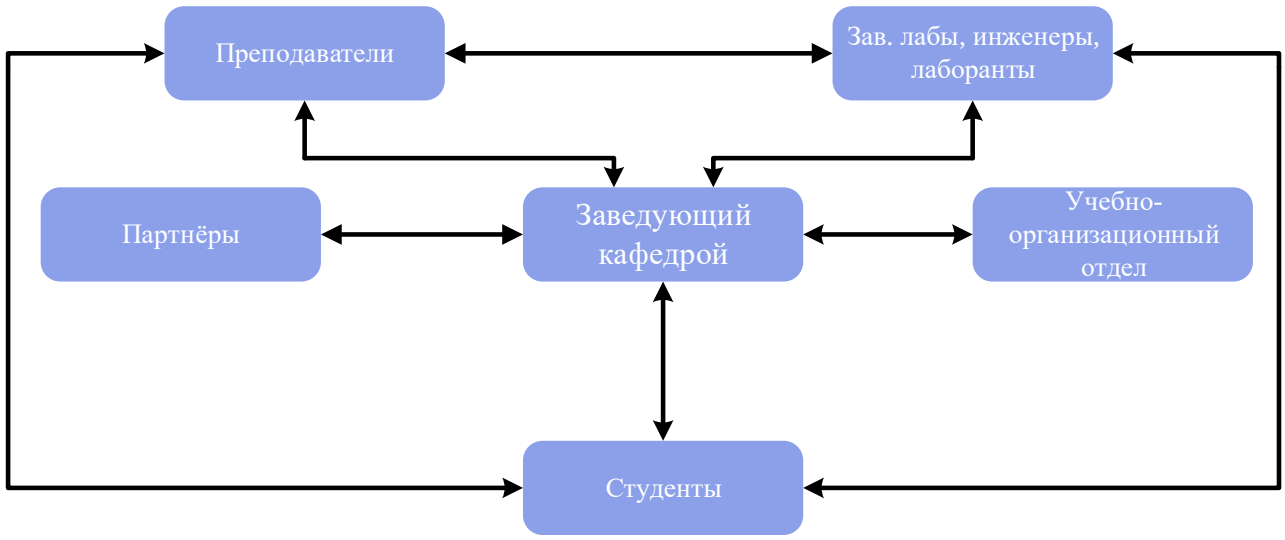

Рисунок 1. Схема информационных потоков кафедры ИСТ

Т. 10. №3. 2024
https://doi.org/10.33619/2414-2948/100

Все эти информационные потоки требуют эффективной системы обработки, передачи и хранения информации, а также обеспечения безопасности данных.

Материал и методы исследования

Методологическую базу исследования составил теоретический анализ нормативных документов и публикаций по теме исследования, а таже наблюдение, беседы, изучение мнение участников образовательного процесса в вузе и обобщение опыта работы по защите информационных потоков, применяемых на кафедре информационных систем и технологий Нижнекамского химико-технологического института и других структурных подразделений вуза.

Результаты и обсуждение

На основании Методического документа «Методика оценки угроз безопасности информации» (https://kurl.ru/VufeG) удалось составить модель нарушителя и модель возможных угроз безопасности информации информационной системы кафедры, на примере электронной информационно-образовательной среды (ИОС): https://moodle.nchti.ru/

Данная ИОС содержит информацию о студентах и преподавателях, а также о курсах, на которых обучаются студенты и с которыми работают преподаватели. В личном кабинете есть всё необходимое для комфортного обучения студентов: прикреплённые лекции, тестовые и практические задания, видео-лабораторные работы и вся информация о них, различная литература и хрестоматия в электронном виде. Для преподавателей также созданы комфортные условия. Они могут настраивать свои курсы, добавлять информацию о курсе и прикреплять все необходимые файлы, а также их редактировать.

Для этой информационной системы в институте выделен отдельный сервер. У администратора есть огромные возможности по управлению информационной системой. Он может создавать новые учётные записи пользователей и добавлять всю необходимую информацию о них. Сама ИОС имеет гибкую настройку, что является положительным моментом при работе с ней.

Среди наиболее опасных угроз информационной безопасности кафедры ИСТ нам удалось выделить:

1) слив персональных данных сотрудников кафедры;

2) внедрение вредоносного ПО;

3) проведение компьютерных атак на оборудование (сервер) и информационные ресурсы;

4) утечка информации по техническим каналам;

5) угроза обесточивания или физического отключения средств хранения, обработки и передачи информации;

6) утечка информации во время взлома электронной почты сотрудников кафедры или информационной системы Moodle.nchti.ru;

7) потеря или кража информации на съёмных носителях (флешка, внешний жёсткий диск).

В Таблице 1 продемонстрированы угрозы, их последствия, а также возможные нарушители данной угрозы.

При сопоставительном анализе данных угроз в сфере информационной безопасности выявлена необходимость постоянного обновления и улучшения системы защиты данных.

Т. 10. №3. 2024
https://doi.org/10.33619/2414-2948/100

Таблица 1

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ИХ ПОСЛЕДСТВИЯ

Наименование угрозы	*Последствия*	*Возможные нарушители*
1.Слив персональных данных (ПД) сотрудников кафедры	Незаконное использование слитой информации. Административная, гражданская или уголовная ответственность для тех сотрудников, кто допустил утечку ПД сотрудников. Институту грозит штраф в размере, который назначит Роскомнадзор.	Любой нарушитель, указанный в модели нарушителя.
2.Внедрение вредоносного программного обеспечения (ПО)	Распространение вируса в корпоративной сети может привести к незначительному повышению объёма сетевого трафика, а также к полному отказу в работе корпоративной сети или к потере критически важных данных. Возможный слив ПД сотрудников через вредоносное ПО, а также выведение из строя всего оборудования.	Разработчики ПО, взломщики программного обеспечения (ПО) и информационных систем (ИС), сотрудники кафедры из-за неосторожности.
3.Проведение компьютерных атак на оборудование (сервер) и информационные ресурсы	Поломка оборудования, и как следствие, потеря важных данных кафедры, а возможно и института. Намеренное искажение информации и ее утечка. Слив ПД сотрудников.	Взломщики ПО и ИС, конкуренты, провайдеры.
4.Утечка информации по техническим каналам	Нарушение конфиденциальности информации и её использование в корыстных целях.	Конкуренты, бывшие сотрудники вуза, сотрудники кафедры.
5. Угроза обесточивания или физического отключения средств хранения, обработки и передачи информации	Поломка оборудования, и как следствие, потеря важных данных кафедры. Слив ПД сотрудников.	Администратор ИС, обслуживающий персонал.
6.Утечка информации во время взлома электронной почты сотрудников кафедры или информационной системы Moodle. nchti.ru.	Незаконное использование полученной информации и утечка ПД сотрудников. Потеря доступа ко всем интернет-ресурсам пользователя.	Взломщики ПО и ИС, конкуренты.
7.Потеря или кража информации на съемных носителях (флешка, внешний жёсткий диск)	Утечка ПД сотрудников и конфиденциальной информации кафедры, а также незаконное использование полученной информации.	Обслуживающий персонал, сотрудники кафедры, студенты.

Кафедра активно работает в данном направлении, осведомляя студентов и сотрудников о необходимости защиты информации со всех сторон. При этом для обеспечения сетевой безопасности нами в рамках исследования выделены четыре основных принципа: 1) защита оборудования; 2) отказоустойчивость оборудования и возможность его быстрого восстановления; 3) мониторинг всей инфраструктуры кафедры для обнаружения уязвимых точек; 4) мониторинг пропускной способности сетевого канала с целью блокировки нежелательного трафика.

Т. 10. №3. 2024
https://doi.org/10.33619/2414-2948/100

Использование вышеперечисленных принципов повышает защиту сети кафедры и обеспечивает безопасность её данных. На Рисунке 2 показана схема сетевого взаимодействия кафедры ИСТ с ЛВС НХТИ и КНИТУ.

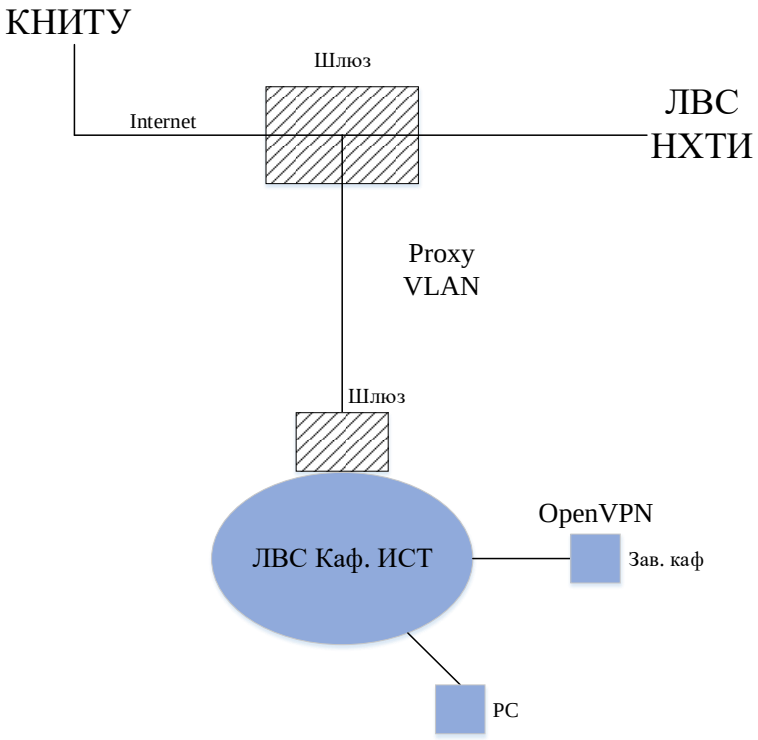

Рисунок 2. Схема сетевого взаимодействия кафедры ИСТ

Управление доступом является одним из основных механизмов защиты информации в компьютерной системе. Для кафедры ИСТ в нашем вузе лучше подходит дискреционная политика доступа, тогда как информационной системе Moodle.nchti.ru подойдёт ролевая модель доступа. На Рисунке 3 изображена схема ролевой политики доступа информационной системы Moodle.nchti.ru., в которой имеется определенный пользователь со своей ролью, где ему разрешены некоторые действия в информационной системе.

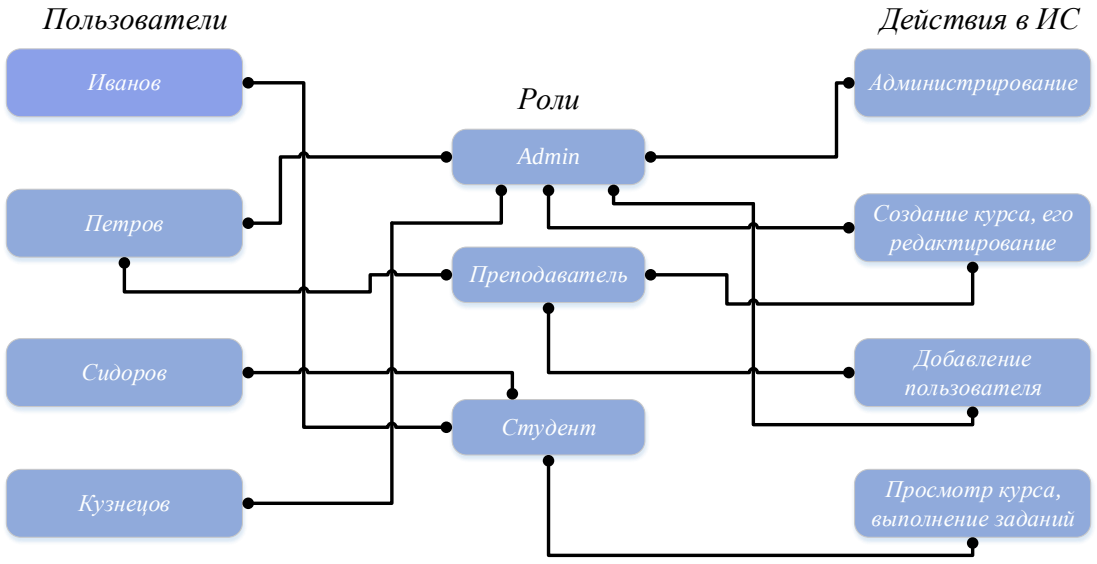

Рисунок 3. Схема ролевой политики доступа кафедры ИСТ

Т. 10. №3. 2024
https://doi.org/10.33619/2414-2948/100

Примером дискреционной политики доступа является мандатное управление, когда расписывается доступ к файлу, где указывается следующие правила доступа (просмотр, запись, чтение), а также операции управления правами доступа (владение, создание, удаление) [2, с. 237].

Данную политику доступа визуально можно показать, используя матрицу доступа. Пример такой матрицы показан в Таблице 2.

Таблица 2

МАТРИЦА ДОСТУПА

Пользователь	*Файл 1*	*Файл 2*	*Файл 3*	*Файл 4*
Иванов	orw	-	-	-
Петров	r	r	rwa	-
Сидоров	rwa	-	orw	r

Условные обозначения: o – возможность передачи прав доступа другим пользователям; r – чтение; w – запись; a – управление информацией

Настройки каждой политики доступа можно прописать в так называемом bat-file. Bat file – это файл, который содержит политику доступа к определенным ресурсам или файлам. Он может устанавливать права доступа для определенных пользователей или групп пользователей, а также ограничивать доступ к конфиденциальной информации.

Заключение

В целом, для обеспечения эффективной безопасности сетевой инфраструктуры кафедры можно использовать различные технические средства, такие как межсетевые экраны, прокси-серверы, внедрение системы мониторинга сетевого трафика, активизацию средств защиты от целевых атак одновременно с выявлением и предотвращением угроз взлома.

Рассмотренные в нашем исследовании примеры реализации ролевой политики доступа демонстрируют ее практическую возможность использования в учебном процессе вуза. В настоящее время для обеспечения информационной безопасности кафедра использует комплексный подход, куда входит использование антивирусного программного обеспечения, определенной политики доступа и прочие технические меры.

Благодарности: Авторы выражают благодарность сотрудникам кафедры информационных систем и технологий Нижнекамского химико-технологичекого института (филиал) ФГБОУ ВО «КНИТУ», а также руководству вуза за возможность апробации приемов по обеспечению безопасности информационных потоков кафедры.

Список литературы:

1. Аль-Хаммуд Ибрахим. Модели и алгоритмы повышения уровня информационной безопасности корпоративных информационно-телекоммуникационных сетей: автореф. дисс. … канд. техн. наук. Владимир, 2007. 16 с.

2. Лиманова Н. И., Анашкин А. С. Основные принципы работы защищенных информационных систем // Бюллетень науки и практики. 2023. Т. 9. №2. С. 235-238. https://doi.org/10.33619/2414-2948/87/27

References:

1. Al'-Khammud, Ibrakhim (2007). Modeli i algoritmy povysheniya urovnya informatsionnoi bezopasnosti korporativnykh informatsionno-telekommunikatsionnykh setei: avtoref. diss. … kand. tekhn. nauk. Vladimir. (in Russian).

2. Limanova, N., & Anashkin, A. (2023). Basic Principles of Secure Information Systems. *Bulletin of Science and Practice, 9*(2), 235-238. (in Russian). https://doi.org/10.33619/2414-2948/87/27

Работа поступила
в редакцию 19.01.2024 г.

Принята к публикации
24.01.2024 г.

Ссылка для цитирования:

Дозморов К. М., Яковлева Е. В. Обеспечение безопасности информационных потоков кафедры в вузе // Бюллетень науки и практики. 2024. Т. 10. №3. С. 513-519. https://doi.org/10.33619/2414-2948/100/67

Cite as (APA):

Dozmorov, K., & Yakovleva, E. (2024). Ensuring the Security of Information Flows at University Departments. *Bulletin of Science and Practice, 10*(3), 513-519. (in Russian). https://doi.org/10.33619/2414-2948/100/67