ОРГАНИЗАЦИЯ СИСТЕМЫ КОНТРОЛЯ ДОСТУПА В ВУЗАХ РФ

Галкова Екатерина Александровна
Специалист отдела технической защиты информации
ООО «Лоджикал АйТи»

Даньшина Марина Владимировна
Заместитель декана факультета Информационных технологий
Московского политехнического университета

Аннотация: *В статье рассмотрена организация системы контроля до-ступа на предприятие. Рассмотрены методы защиты обеспечения безопасно-сти на предприятии и разработаны рекомендации по усовершенствованию данной системы.*

Ключевые слова: *обеспечение безопасности, предприятие, информа-ционные технологии, СКУД.*

Abstract: *The article describes the organization of the access control system in the enterprise. Examines the methods of ensuring security in the enterprise and recommendations for an improved system.*

Keywords: *security, enterprise, information technology, access control.*

Введение. В современном мире информация очень важна на любом предприятии. Большую роль в деятельности организации играет эффективное использование информации, ее безопасное хранение и передача, так как все это сказывается на прибыли и развитии предприятия. Сейчас большинство документов и данных представлены в электронном виде, что удобно, но в тоже время очень небезопасно. Комплексная система защиты информации (КСЗИ) – представляет собой организационные и инженерно-технические мероприятия для защиты информации от нарушения целостности, конфиденциальности и доступности.

Современные вузы владеют большим объемом данных, которые содержат разнообразную информацию такую как: персональные данные учащихся, преподавателей и иных сотрудников, учебные планы, финансовые документы, важные документы по проектам и исследованиям. Вузы являются небезопасными объектами, так как они являются публичными помещениями, в которых преобладает непостоянная аудитория.

Цель исследования: Проанализировать безопасность системы контроля доступа в вузах РФ.

Задачи исследования:

Изучить системы контроля доступа на предприятие и их организацию.

Определить важность обеспечения защиты безопасности в вузе.

Рассмотреть методы обеспечения защиты безопасности в вузе.

Система контроля и управления доступом (СКУД) это система, состоящая из программно-технического оборудования и ряда мероприятий, проводимых для автоматизации пропуска сотрудников на территорию защищаемого объекта. [1]

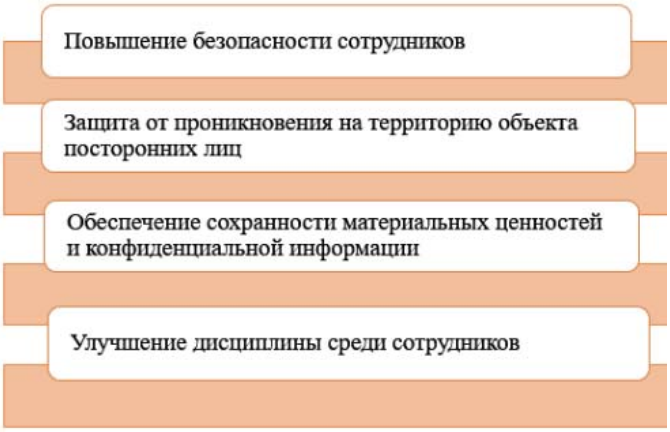

Рисунок 1. Причины установки СКУД на предприятии

Причины внедрения системы контроля и управления доступом на предприятие представлены на рисунке 1.

При формировании СКУД выделяют точки и зоны доступа. Точки доступа — это места, где проверяется идентификатор пользователя на право этого лица находиться на охраняемом объекте. В качестве идентификатора могут выступать: ключи, карточки и коды. Точки доступа представляют собой турникеты, шлагбаумы, двери, которые оснащены специальными замками. В зависимости от требований к безопасности и расположения на объекте охраняемых помещений такие точки доступа могут находиться в различных местах защищаемой территории. [2]

Системы контроля и у правления доступом, установленные в помещениях дают возможности, представленные на рисунке 2.

Рисунок 2. Возможности СКУД

Системы контроля и у правления доступом востребованы во многих отраслях. На рисунке 3 отображено, где наиболее востребованы СКУД:

В работе СКУД используются компоненты, которые представлены на рисунке 4.

В зависимости от масштабов защищаемого объекта сложность и размер внедряемой системы контроля доступа могут варьироваться.

Одна из самых важных задач в организации и внедрении СКУД в систему вуза - использование информационных технологий. Во-первых, это необходимо для выполнения требований криминальной безопасности, так как в стране наблюдается рост преступности и угроз террористических актов. Во-вторых, необходимо запретить проход посторонних в ряд помещений, а также вести учет рабочего времени и контролировать посещаемость студентов в реальном времени. Кроме того, вузы, использующие современные информационные технологии, имеют высокий престиж.

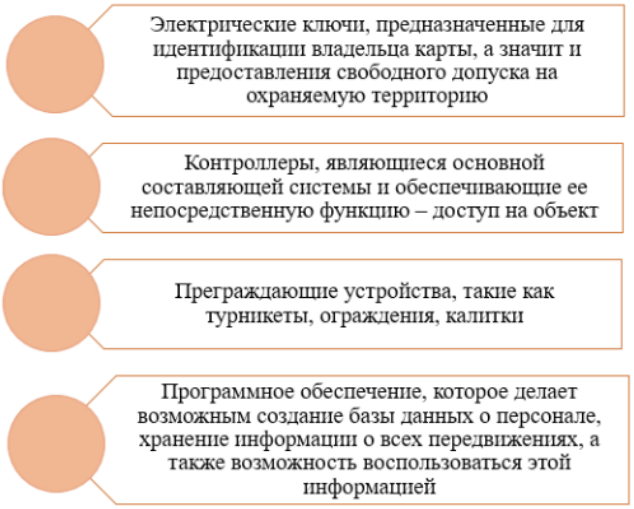

Рисунок 4. Компоненты СКУД

Каждый сотрудник и учащийся имеет свой уникальный идентификатор. Он позволяет проходить на территорию вуза, а также проходить в некоторые помещения с ограниченным допуском. [3]

Наиболее часто идентификатор имеет форму пластиковой карты с магнитной полосой, на которую записана персональная информация сотрудника или учащегося. Чтобы получить доступ на территорию или в помещение для ограниченного количества лиц, собственник карточки должен поднести ее к считывающему устройству, после чего контроллер позволяет ему пройти на охраняемый объект. Тем не менее такой идентификатор может замедлять проход на территорию с большим числом сотрудников и учащихся, так как на прикладывание карты уходит некоторое время. В этом случае можно использовать современные радиочастотные бесконтактные Proximity-карты или брелоки Touch Memory, кото-

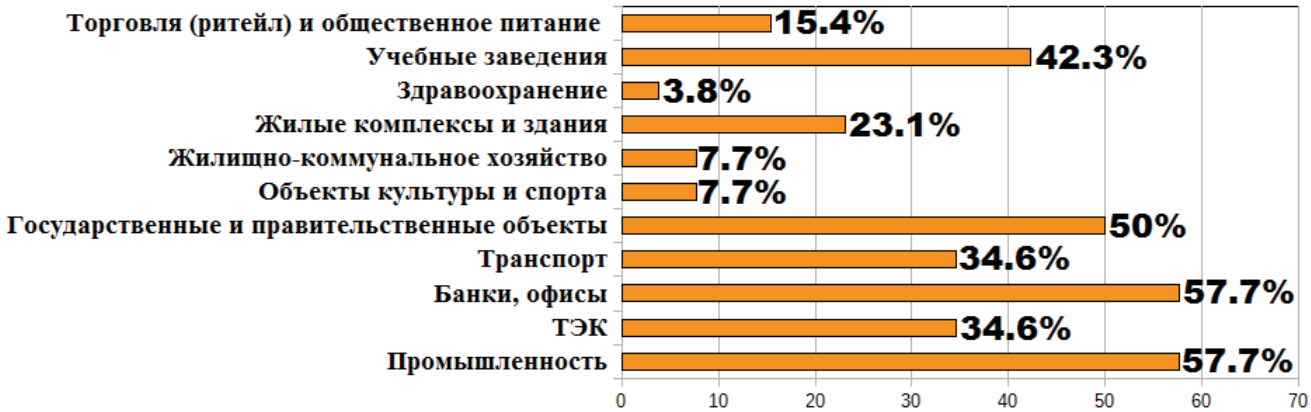

Рисунок 3. Востребованность СКУД в отраслях

рые представляют собой металлическую таблетку с чипом внутри. В новых системах контроля доступа используется дополнительная идентификация по фото владельца. Наиболее часто сегодня применяются биометрические сканеры отпечатков пальцев, картридеры и клавиатуры для набора ПИН-кода.

Вывод. СКУД стали частью современной корпоративной культуры. С помощью системы контроля и управления доступом решается достаточно много задач: создание пропускного режима на территорию вуза, в аудитории, лаборатории, другие помещения с ограниченным доступом, а также в общежития, учет рабочего времени преподавателей, контроль посещаемости студентов. Внедрение такой системы является дополнительным гарантом безопасности вуза, что очень важно в современном мире.

Список литературы

1. Тюменев А.В. Обеспечение безопасности информационных ресурсов предприятия/Тюменев А.В., Панов Н.Н./Системные технологии. 2017. № 3 (24). С. 68-71.
2. Системы контроля и управления доступом (СКУД) http://www.prom-seti.ru/lmenu/sistemy-kontrolya-i-upravleniya-dostupom-skud/
3. Александр Красноцветов Особенности создания СКУД в вузах/ ТЗ №3-2010 г.

ОБЕСПЕЧЕНИЕ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Вершинина Дарья Дмитриевна
Специалист отдела технической защиты информации
ООО «Лоджикал АйТи»

Тюменев Александр Владимирович
Подполковник полиции, начальник управления комплексной безопасности Московского политехнического университета

Аннотация: *В статье рассмотрено комплексное обеспечение безопасности предприятия. Особое место уделено физическим методам защиты. Рассмотрены механизмы, используемые для защиты контролируемой зоны организации. Использование комплексной системы позволяет успешно функционировать в нестабильных условиях внешней и внутренней среды.*

Ключевые слова: *безопасность, информационная безопасность, защита, методы.*

Abstract: *This article describes the comprehensive security of the enterprise. A special place is given to physical methods of protection. The mechanisms used to protect the controlled area of the organization are considered. The use of an comprehensive system allows you to successfully operate in unstable condi-tions of external and internal environment.*

Keywords: *security, information security, protection, methods.*

Введение. В современном мире важнейшим ресурсом является информация. Множество предприятий каждый день обрабатывают данные различных видов, которые несут огромную значимость для компании. Информационную безопасность предприятия определяет используемая им информационная технология, являющаяся в виде информационного процесса, производимого на рассортированных по контролируемой зоне организации технических средств; а также наличие мест доступа или утечки информации, создающих потенциальную возможность осуществления угроз; и наличие действенных средств защиты. Одной из наиболее важных составляющих комплексной безопасности организации является физическая защита.

Цель исследования: Изучить обеспечения безопасности предприятия.

Задачи исследования:

- Проанализировать обеспечение безопасности на предприятии России.
- Рассмотреть физическую безопасность предприятия.
- Разработать рекомендации по усовершенствованию комплексной безопасности на