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

предприятии.

Главной целью комплексной системы защиты информации является обеспечение непрерывности бизнеса и предотвращение угроз его безопасности. Для непрерывной работы предприятия необходимо защищать информационную систему от возникающих угроз, чаще всего угрозой является физическое лицо и его действия в отношении информационной системы, последствия которых могут быть катастрофическими. Примером этого является: хищение имущества или персональных данных, а также создание непредвиденных ситуаций на объекте. На базе принципов «разумной достаточности», «эффективность – стоимость» строится безопасность любой организации, также она должна базироваться на тщательно проработанной концепции физической безопасности на предприятии. Согласно статистике больше 80% организаций подвержены нарушениям безопасности данных, что привело к финансовым убыткам. [1]

Анализируя информационные атаки можно выделить слабые места в обеспечении безопасности информационных ресурсов предприятия. Наиболее встречаемая это утечка информации к конкурентам, потеря данных, передача в чужие руки конфиденциальной информации компании – все это несет большой риск для предприятия. Результаты исследования представлены на рисунке 1.

Физическая безопасность (защиты) организации – это совокупность правовых норм, организационных мер и инженерно-технических решений, направленных на защиту важных интересов и ресурсов предприятия (объекта) от угроз злоумышленных противоправных действий физических лиц (нарушителей). [2]

Методы защиты представлены на рисунке 2.

Препятствие – данные средство подразумевает использование физических барьеров для защиты информации от мошеннических действий. Реализуется путем запрета к носителям информации и аппаратуре.

Маскировка – способ защиты информации, использующий шифрование данных в автоматизированной системе (АС).

Управление доступом - метод, базирующийся на разграничении доступа к информации. Позволяет регулировать степень доступа в зависимости от выполняемых функций в организации.

Регламентация – метод, предполагающий, что при незаконном запросе злоумышленника доступ к хранению и передаче данных будет минимален.

Побуждение - метод, основанный на принятых в обществе правилах, стимулирующий не нарушать запрет на использование конфиденциальной информации.

Принуждение – метод, обязывающий пользователей при доступе к конфиденциальной информации соблюдать определенный регламент (правила). Нарушение влечет материальную, административную или уголовную ответственность.

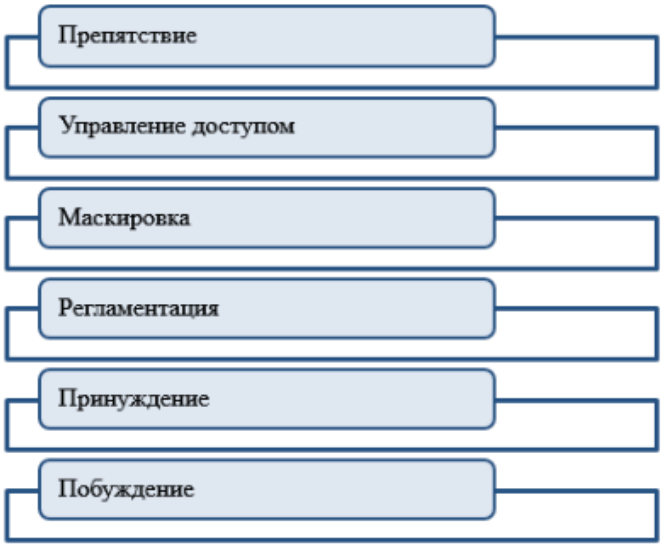

Рисунок 2. Методы физической защиты информации

Выше описанные методы защиты обеспечивают максимальный уровень безопасности всей информационной системы предприятия.

Рассмотрим один из защитных механизмов:

Физические средства защиты нужны для качественной организации внешней охраны и наблюдения за контролируемой зоной, а также для защиты автоматизированной информационной системы. На предприятии представлены в виде специальных технических устройств.

Структурная схема типовой системы физической

Рисунок 1. Атаки на предприятие

защиты приведена на рисунке 3.

Рисунок 3. Система физической безопасности предприятия

Обычно в организации используются механические системы. Наряду с ними внедряются электронные АС физической защиты. Под электронной системой понимается защита территории объекта, пожарная безопасность, охрана помещений, пропускной режим, наблюдение и устройства сигнализации.

После анализа уязвимостей объекта, которые являются важнейшей задачей на стадии проектирования, следует разработать рекомендации по обеспечению безопасности.

Для предотвращения несанкционированного доступа к защищаемой информации через электромагнитные каналы используют специальные устройства и материалы, которые обладают свойствами поглощать и предохранять от посторонних воздействий:

- Экранирование всех поверхностей в помещении – пола, стен и потолка с помощью металлизированных панелей.
- Оконные проемы оборудуют жалюзи с металлической нитью или покрывают стекла токопроводящим составом;
- На все отверстия в помещениях устанавливают металлические сетки с системой заземления или соединяют с настенной экранировкой;
- В вентиляционные каналы устанавливают аудиоизлучатели, блокирующие распространение радиоволн;
- Применяют шумовые генераторные устройств для предотвращения утечки информации по каналам ПЭМИН (Побочные электромагнитные излучения и наводки), а также для защиты от закладных подслушивающих устройств.

Защита всего информационного оборудования организации, а также переносных устройств (магнитных лент или флеш-накопителей) осуществляется с помощью механизмов изображенных на рисунке 4:

Рисунок 4. Механизмы защита информационного оборудования и переносных устройств

- Замки (механические, радиоуправляемые, кодовые, с чипом), которые желательно поставить на сейфы, системные блоки, оконные блоки, двери и другие устройства;
- Инерционные датчики - используются в электросети, телефонных проводах, телекоммуникационных антеннах, который искажает частоту измеряемого сигнала;
- Микровыключатели - устройства дистанционного управления, которые фиксируют открывание и закрывание окон и дверей;
- Акустомагнитные этикетки/наклейки - приклеивают на приборы, документы, системные блоки, узлы для защиты от выноса за контролируемую зону организации или помещения. При попытке выноса злоумышленником документов или устройств, имеющих данную этикетку, через пропускные устройства звучит сигнал тревоги.
- Специальные сейфы и шкафы из метала, в которые устанавливают серверы, принтеры и другие переносные устройства.

Схема использования механизмов защиты приведена на рисунке 5.

Блоки и узлы автоматизированной системы требуют особой защиты. Для это применяют:

- Экранированный кабель, который будет монтироваться внутри и снаружи стен;

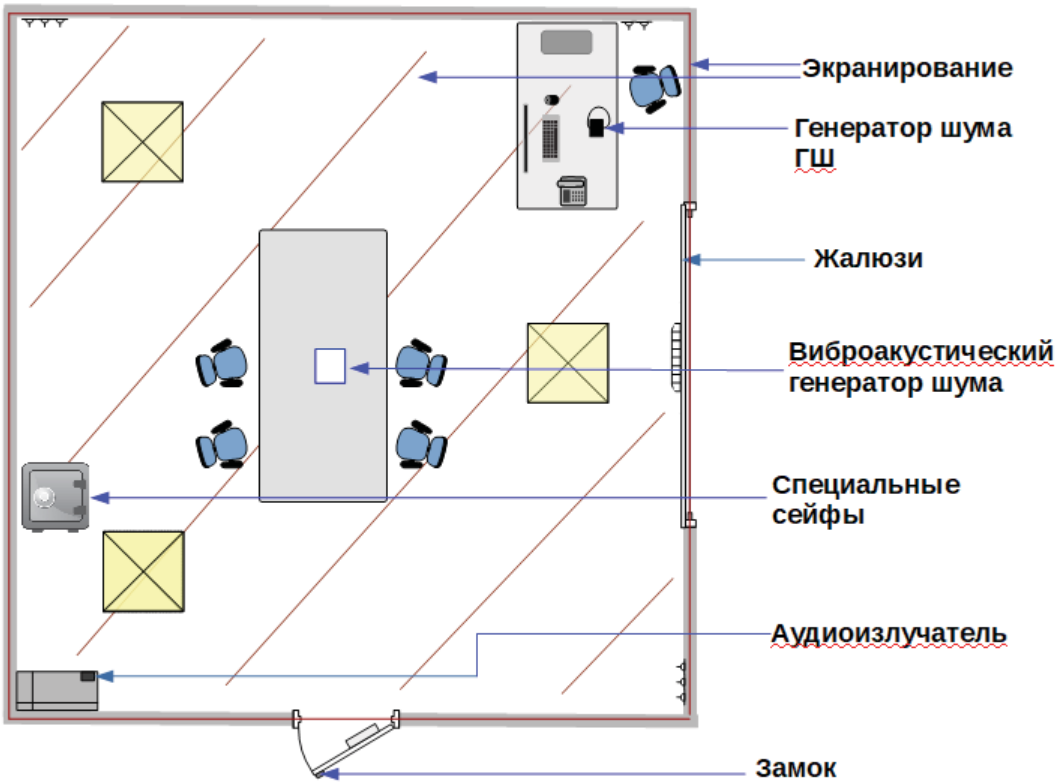

Рисунок 5. Схема помещения

- Сетевые фильтры, которые не пропускают электромагнитные излучения;
- Провода, дроссели, наконечники, конденсаторы и другие устройства, которые имеют помехоподавляющее действие;
- Диэлектрические разделительные вставки, которые устанавливают на водопроводные и газовые трубы для разрывания электромагнитной цепи.

Не все описанные методы являются оптимальными:

- Для обнаружения подслушивающих устройств самым продуктивным является использование рентгена. Рентгеновское обследование имеет и свои минусы: оно самое дорогостоящее, а также наносит вред здоровью человека.
- Генераторы шума, действующие методом снятия излучений с дисплея, также отрицательно сказываются на здоровье. Таким образом, данное устройство защиты применяется достаточно редко на практике.

Вывод. В условиях современного рынка необходимо внедрять все выше описанные методы и механизмы защиты для предотвращения несанкционированных угроз безопасности. Способы и виды взломов и нападений на конфиденциальные данные постоянно совершенствуются и поэтому необходимо регулярно проверять и обновлять защитную систему предприятия и быть в курсе новых угроз и методов борьбы с ними.

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. В. Л. Шульц, А. Д. Рудченко, А. В. Юрченко. Безопасность пред-принимательской деятельности/ Учебник для академического бакалавриа-та// М. : Издательство Юрайт, 2017. — 237 с.