УДК 004

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ДАННЫХ ИНФОРМАЦИОННОЙ СИСТЕМЫ НА ПРЕДПРИЯТИЕ

Додонова Ю.П., студентка 3 курса экономического факультета
Научный руководитель – Голубев С.В., к.э.н, доцент
ФГБОУ ВО Ульяновский ГАУ

Ключевые слова: *информационная безопасность, целостность данных, вирус, компьютерные преступления.*

Сегодня многие российские компании решают задачи создания системы информационной безопасности, которая соответствовала бы «лучшим практикам» и стандартам в области информационной безопасности и отвечала современным требованиям защиты информации по параметрам конфиденциальности, целостности и доступности.

В общем понятии информационная безопасность - это состояние защищенности информации. Информационная безопасность создает условия формирования безопасного состояния информационной среды общества, его использование и развитие в интересах граждан, предприятий и даже государства.

Для каждого современного предприятия, компании или организации одной из самых главных задач является именно обеспечение информационной безопасности. Когда предприятие стабильно защищает свою информационную систему, оно создает надежную и безопасную среду для своей деятельности. Повреждение, утечка, неимение и кража информации — это всегда убытки для каждой компании. Например, могут появиться убытки от плохой репутации компании, от отсутствия клиентов, от затрат на возобновление стабильной работы или от потери важной информации, которой располагала данная компания.

На данный момент сформулировано три базовых задачи, которые должна обеспечивать информационная безопасность:

- Целостность данных - защита от сбоев, ведущих к потере информации, а также защита от незаконного создания или уничтожения данных. Примером нарушения целостности данных является повреждение бухгалтерских баз, в дальнейшем это повлечет за собой последствия, которые определенно станут негативными для компании.

- Конфиденциальность информации - незаконное разглашение, утечка, повреждение информации;
- Доступность информации для всех пользователей - отказ в обслуживании или услугах, которые могут быть вызваны вирусной активностью или действиями злоумышленников.

Нарушение одного из этих аспектов может привести к невозможности нормальной работы предприятия. На наличие любого из нарушений могут повлиять и внутренние, и внешние угрозы. Учитывая сегодняшнее развитие информационного общества, можно сделать вывод о тенденции к росту количества угроз безопасности.

Полноценная информационная безопасность компаний предполагает постоянный контроль всех существенных событий и состояний, которые влияют на надежность защиты информации. Причем, защита обязана осуществляться постоянно и охватывать весь жизненный цикл данных, то есть от ее поступления или создания до уничтожения или утраты важности и актуальности.

Основными факторами, оказывающими влияние на защиту информации и данных на предприятии, являются:

- Приумножение сотрудничества компании с партнерами;
- Автоматизация бизнес-процессов;
- Тенденция к росту объемов информации предприятия, которая передается по доступным каналам связи;
- Тенденция к росту компьютерных преступлений.
- Информационная защита предприятия определяется целым сочетанием предпринимаемых мер, которые направлены на безопасность важной информации. Эти меры можно разделить на две группы:
- Организационные меры;
- Технические меры.

Организационные меры заключаются в формальных процедурах и правилах работы с важной информацией, информационными сервисами и средствами защиты.

Технические меры включают в себя использование программных средств контроля доступа, мониторинг утечек и краж информации, антивирусную защиту, защиту от электромагнитных излучений и т. д.

Задачи систем информационной безопасности компании многогранны. К примеру, это обеспечение надежного хранения данных на различных носителях; защита информации, передаваемой по каналам

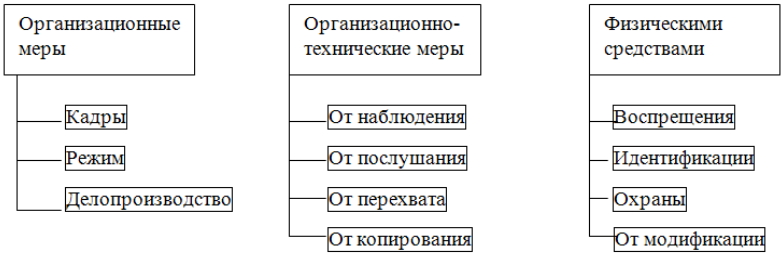

Рисунок 1 - Организационные меры информационной защиты информации

Рисунок 2 - Технические меры информационной защиты информации

связи; ограничение доступа к некоторым данным; создание резервных копий и другое.

Полноценное обеспечение информационной безопасности компании реально только при правильном подходе к защите данных. В системе информационной безопасности нужно учитывать все актуальные на сегодняшний день угрозы и уязвимости.

Библиографический список

1. Определение информационной безопасности [Электронный ресурс].- Режим доступа: URL: http://www.itspecial.ru/opredelenie_informacionnoi_bezopasnosti.html. Дата обращения 16.04.2017.
2. Угрозы информационной безопасности в АС [Электронный ресурс].- Режим доступа. — URL: http://asher.ru/security/book/its/05. Дата

обращения 16.04.2017.

SECURITY DATA INFORMATION SYSTEMS IN THE ENTERPRISE

Dodonova Y.P.

Key words: *information security, data integrity, virus, computer crime.*

Today, many Russian companies solve the problem of creation of system of information security, which would be consistent with "best practices" and standards in the field of information security and meet the modern requirements of information protection in the parameters of confidentiality, integrity and availability.