В связи с развитием информационных технологий и компьютеризацией экономики одним из важнейших вопросов в деятельности компании становится обеспечение информационной безопасности.

Информация – это один из самых ценных и важных активов любого предприятия и должна быть надлежащим образом защищена.

Рудинский Виктор Валерьевич,
заместитель директора по ИКТ ОГБОУ «Центр образования для детей с особыми образовательными потребностями г. Смоленска»

rudinskiy@internet.ru

Рудинский Виктор Валерьевич
Подписано цифровой подписью: Рудинский Виктор Валерьевич

Информационная безопасность — это сохранение и защита информации, а также ее важнейших элементов, в том числе системы и оборудование, предназначенные для использования, сбережения и передачи этой информации. Другими словами, это набор технологий, стандартов и методов управления, которые необходимы для защиты информационной безопасности.

Цель обеспечения информационной безопасности — защитить информационные данные и поддерживающую инфраструктуру от случайного или преднамеренного вмешательства, что может стать причиной потери данных или их несанкционированного изменения. Информационная безопасность помогает обеспечить непрерывность бизнеса.

Для успешного внедрения систем информационной безопасности на предприятии необходимо придерживаться трех главных принципов:

1. **Конфиденциальность**. Это значит ввести в действие контроль, чтобы гарантировать достаточный уровень безопасности с данными предприятия, активами и информацией на разных этапах деловых операций для предотвращения нежелательного или несанкционированного раскрытия. Конфиденциальность должна поддерживаться при сохранении информации, а также при транзите через рядовые организации независимо от ее формата.

2. **Целостность**. Целостность имеет дело с элементами управления, которые связаны с обеспечением того, чтобы корпоративная информация была внутренне и внешне последовательной. Целостность также гарантирует предотвращение искажения информации.

3. **Доступность**. Доступность обеспечивает надежный и эффективный доступ к информации уполномоченных лиц. Сетевая среда должна вести себя предсказуемым образом с целью получить доступ к информации и данным, когда это необходимо. Восстановление системы по причине сбоя является важным фактором, когда речь идет о доступности информации, и такое восстановление также должно быть обеспечено таким образом, чтобы это не влияло на работу отрицательно.

Выбор и внедрение подходящих видов контроля безопасности поможет организации снизить риск до приемлемых уровней. Выделяют следующие виды контроля:

1. **Административный**. Административный вид контроля состоит из утвержденных процедур, стандартов и принципов. Он формирует рамки для ведения бизнеса и управления людьми. Законы и нормативные акты, созданные государственными органами, также являются одним из видов административного контроля. Другие примеры административного контроля включают политику корпоративной безопасности, паролей, найма и дисциплинарные меры.

2. **Логический**. Логические средства управления (еще называемые техническими средствами контроля) базируются на защите доступа к информационным системам, программном обеспечении, паролях, брандмауэрах, информации для мониторинга и контроле доступа к системам информации.
3. **Физический**. Это контроль среды рабочего места и вычислительных средств (отопление и кондиционирование воздуха, дымовые и пожарные сигнализации, противопожарные системы, камеры, баррикады, ограждения, замки, двери и др.).

Угрозы информационной безопасности

Угрозы информационной безопасности можно разделить на следующие:

- Естественные (катаклизмы, независящие от человека: пожары, ураганы, наводнение, удары молнии и т.д.).

- Искусственные, которые также делятся на:
  — непреднамеренные (совершаются людьми по неосторожности или незнанию);
  — преднамеренные (хакерские атаки, противоправные действия конкурентов, месть сотрудников и пр.).

- Внутренние (источники угрозы, которые находятся внутри системы).

- Внешние (источники угроз за пределами системы)

Так как угрозы могут по-разному воздействовать на информационную систему, их делят на пассивные (те, которые не изменяют структуру и содержание информации) и активные (те, которые меняют структуру и содержание системы, например, применение специальных программ).

Наиболее опасны преднамеренные угрозы, которые все чаще пополняются новыми разновидностями, что связано, в первую очередь, с компьютеризацией экономики и распространением электронных транзакций. Злоумышленники не стоят на месте, а ищут новые пути получить конфиденциальные данные и нанести потери компании.

Чтобы обезопасить компанию от потери денежных средств и интеллектуальной собственности, необходимо уделять больше внимания информационной безопасности. Это возможно благодаря средствам защиты информации в лице передовых технологий.

Средства защиты информационной безопасности

Средства защиты информационной безопасности — это набор технических приспособлений, устройств, приборов различного характера, которые препятствуют утечке информации и выполняют функцию ее защиты.

Средства защиты информации делятся на:

- **Организационные**. Это совокупность организационно-технических (обеспечение компьютерными помещениями, настройка кабельной системы и др.) и

организационно-правовых (законодательная база, статут конкретной организации) средств.

- **Программные**. Т.е. программы, которые помогают контролировать, хранить и защищать информацию и доступ к ней.

- **Технические (аппаратные)**. Это технические виды устройств, которые защищают информацию от проникновения и утечки.

- **Смешанные аппаратно-программные**. Выполняют функции как аппаратных, так и программных средств.

В связи со стремительным развитием ИТ, все более частыми кибератаками, компьютерными вирусами и другими появляющимися угрозами наиболее распространенными и востребованными на сегодняшний день являются программные средства защиты информации.

Виды средств защиты информации:

- **Антивирусные программы** — программы, которые борются с компьютерными вирусами и возобновляют зараженные файлы.

- **Облачный антивирус (CloudAV)** – одно из облачных решений информационной безопасности, что применяет легкое программное обеспечение агента на защищенном компьютере, выгружая большую часть анализа информации в инфраструктуру провайдера. CloudAV – это также решение для эффективного сканирования вирусов на приспособлениях с невысокой вычислительной мощностью для выполнения самих сканирований. Некоторые образцы облачных антивирусных программ – это Panda Cloud Antivirus, Crowdstrike, Cb Defense и Immunet.

- **DLP (Data Leak Prevention) решения** — это средства защиты от утечки информации. Предотвращение утечки данных (DLP) представляет собой набор технологий, направленных на предотвращение потери конфиденциальной информации, которая происходит на предприятиях по всему миру. Успешная реализация этой технологии требует значительной подготовки и тщательного технического обслуживания. Предприятия, желающие интегрировать и внедрять

DLP, должны быть готовы к значительным усилиям, которые, если они будут выполнены правильно, могут значительно снизить риск для организации.

- **Криптографические системы** — преобразование информации таким образом, что ее расшифровка становится возможной только с помощью определенных кодов или шифров (DES — Data Encryption Standard, AES – Advanced Encryption Standard). Криптография обеспечивает защиту информации и другими полезными приложениями, включая улучшенные методы проверки подлинности, дайджесты сообщений, цифровые подписи и зашифрованные сетевые коммуникации. Старые, менее безопасные приложения, например Telnet и протокол передачи файлов (FTP), медленно заменяются более безопасными приложениями, такими как Secure Shell (SSH), которые используют зашифрованные сетевые коммуникации. Беспроводная связь может быть зашифрована с использованием таких протоколов, как WPA/WPA2 или более старый (и менее безопасный) WEP. Проводные коммуникации защищены с использованием AES для шифрования и X.1035 для аутентификации и обмена ключами. Программные приложения, такие как GnuPG или PGP, могут применяться для шифрования информационных файлов и электронной почты.

- **Межсетевые экраны (брандмауэры или файрволы)** — устройства контроля доступа в сеть, предназначенные для блокировки и фильтрации сетевого трафика. Брандмауэры обычно классифицируются как сетевые или хост-серверы. Сетевые брандмауэры на базе сети расположены на шлюзовых компьютерах LAN, WAN и интрасетях. Это либо программные устройства, работающие на аппаратных средствах общего назначения, либо аппаратные компьютерные устройства брандмауэра. Брандмауэры предлагают и другие функции для внутренней сети, которую они защищают, например, являются сервером DHCP или VPN для этой сети. Одним из лучших решений как для малых, так и для больших предприятий являются межсетевые экраны CheckPoint.

- **VPN (Virtual Private Network)**. Виртуальная частная сеть (VPN) дает возможность определить и использовать для передачи и получения информации частную сеть в рамках общедоступной сети. Таким образом, приложения, работающие по VPN, являются надежно защищенными. VPN дает возможность подключиться к внутренней сети на расстоянии. С помощью VPN можно создать общую сеть для территориально отдаленных друг от друга предприятий. Что касается отдельных пользователей сети – они также имеют свои преимущества использования VPN,

так как могут защищать собственные действия с помощью VPN, а также избегать территориальные ограничения и использовать прокси-серверы, чтобы скрыть свое местоположение.

- **Proxy-server (Прокси-сервер)** – это определенный компьютер или компьютерная программа, которая является связывающим звеном между двумя устройствам, например, такими как компьютер и другой сервер. Прокси-сервер можно установить на одном компьютере вместе с сервером брандмауэра, или же на другом сервере. Плюсы прокси-сервера в том, что его кэш может служить для всех пользователей. Интернет-сайты, которые являются наиболее часто запрашиваемыми, чаще всего находятся в кэше прокси, что несомненно удобно для пользователя. Фиксирование своих взаимодействий прокси-сервером служит полезной функцией для исправления неполадок.

- **Системы мониторинга и управления информационной безопасностью, SIEM**. Чтобы выявлять и реагировать на возникающие угрозы информационной безопасности, используется решение SIEM, которое выполняет сбор и анализ событий из разных источников, таких как межсетевые экраны, антивирусы, IPS, оперативные системы и т.п. Благодаря системе SIEM у компаний появляется возможность централизованно хранить журналы событий и коррелировать их, определяя отклонения, потенциальные угрозы, сбои в работе ИТ-инфраструктуры, кибератаки и т.д.

Отдельное внимание стоит уделять управлению мобильными устройствами на предприятии, так как многие сотрудники часто используют личные смартфоны, планшеты и ноутбуки в корпоративных целях.

Информация очень важна для успешного работы, следовательно, нуждается в соответствующей защите. Особенно актуально это стало в последнее время, когда на передний план вышли информационные технологии. Так как мы живем в эпоху цифровой экономики, без них рост компании просто невозможен.

Информация сейчас подвергается все большему числу угроз и уязвимостей. Хакерские атаки, перехват данных по сети, воздействие вирусного ПО и прочие угрозы приобретают более изощренный характер и набирают огромный темп.

На выбор подходящих средств защиты информации влияют многие факторы, включая сферу деятельности компании, ее размер, техническую сторону, а также знания сотрудников в области информационной безопасности.