ВИДЫ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

EMU доцент **Ш.А.Акбарова**
sohidaakbarova9@gmail.com

Использование компьютерных и информационных систем в экономике, управлении, связи, исследованиях, образовании, услугах, торговле, финансах и других областях человеческой деятельности является ключевым аспектом развития сообщества

Информационная инфраструктура предприятия постоянно подвергается многочисленным угрозам, которые по своему происхождению делятся на несколько видов:

Естественные. Угрозы, вызванные причинами, не зависящими от человека. К их числу относятся ураганы, пожары, удары молнии, наводнения, другие природные катаклизмы.

Искусственные. Комплекс угроз информационной безопасности созданных человеком. Искусственные угрозы, в свою очередь, делят на преднамеренные и непреднамеренные. К преднамеренным угрозам относят действия конкурентов, хакерские атаки, вредительство обиженных работников и т. д. Непреднамеренные угрозы возникают в результате действий, совершенных из-за недостатка компетентности или по неосторожности.

Внутренние. Угрозы, которые возникают внутри информационной инфраструктуры предприятия.

Внешние. Угрозы, которые имеют происхождение за пределами информационной инфраструктуры предприятия.

В зависимости от характера воздействия угрозы информационной безопасности делятся на пассивные и активные. Пассивные угрозы — это факторы воздействия, которые не могут изменять содержание и структуру информации. Активные угрозы способны вносить такие изменения. К их числу относят, например, воздействие вредоносного ПО.

Средствами защиты информации называют устройства, приборы, приспособления, программное обеспечение, организационные меры, которые предотвращают утечку информации и обеспечивают ее сохранение в условиях воздействия всего спектра актуальных угроз.

В зависимости от используемых способов реализации, средства защиты информационной безопасности бывают следующих типов:

Организационные. Комплекс мер и средств организационно-правового и организационно-технического характера. К первым относят законодательные и нормативные акты, локальные нормативные документы организации.

Аппаратные (технические). Специальное оборудование и устройство, предотвращающее утечки, защищающее от проникновения в ИТ-инфраструктуру.

Программные. Специальное ПО, предназначенное для защиты, контроля, хранения информации.

Программно-аппаратные. Специальное оборудование с установленным программным обеспечением для защиты данных.

Наиболее широкое распространение сегодня получили программные средства защиты информации. Они в полной мере отвечают требованиям эффективности и актуальности, регулярно обновляются, эффективно реагируя на актуальные угрозы искусственного характера.

Для защиты данных в современных сетях применяется широкий спектр специализированного программного обеспечения. Можно выделить следующие типы программных средств защиты:

Антивирусное ПО. Специализированный софт для обнаружения, нейтрализации и удаления компьютерных вирусов. Обнаружение может выполняться во время проверок по расписанию или запущенных администратором. Программы выявляют и блокируют подозрительную активность программ в «горячем» режиме. Кроме того, современные антивирусы могут возобновлять файлы, зараженные вредоносными программами.

Облачные антивирусы (CloudAV). Сочетание возможностей современных антивирусных программ с облачными технологиями. К таким решениям относятся сервисы Crowdstrike, Panda Cloud Antivirus, Immunet и многие другие. Весь основной функционал ПО размещен в облаке, а на защищаемом компьютере устанавливается клиент — программа с минимальными техническими требованиями. Клиент выгружает в облачный сервер основную часть анализа данных. Благодаря этому обеспечивается эффективная антивирусная защита при минимальных ресурсных требованиях к оборудованию.

Решения DLP (Data Leak Prevention). Специальные программные решения, предотвращающие утечку данных. Это комплекс технологий, которые эффективно защищают предприятия от потери конфиденциальной информации в силу самых разных причин. Внедрение и поддержка DLP — требует достаточно больших вложений и усилий со стороны предприятия.

Системы криптографии. (DES — Data Encryption Standard, AES — Advanced Encryption Standard). Преобразуют данные, после чего их расшифровка может быть выполнена только с использованием соответствующих шифров. Помимо этого, криптография может использовать другие полезные приложения для защиты информации, в том числе дайджесты сообщений, методы проверки подлинности, зашифрованные сетевые коммуникации, цифровые подписи. Сегодня новые приложения, использующие зашифрованные коммуникации, например, Secure Shell (SSH), постепенно вытесняют устаревающие решения, не обеспечивающие в современных условиях требуемый уровень безопасности, такие как Telnet и протокол передачи файлов FTP.

Межсетевые экраны (МСЭ). Решения, которые обеспечивают фильтрацию и блокировку нежелательного трафика, контролируют доступ в сеть. Различают такие виды файерволов, как сетевые и хост-серверы. Сетевые файерволы размещаются на шлюзовых ПК LAN, WAN и в интрасетях. Межсетевой экран может быть выполнен в

формате программы установленной на обычный компьютер или иметь программно-аппаратное исполнение.

Виртуальные частные сети VPN (Virtual Private Network). Решение, использующее в рамках общедоступной сети частную сеть для передачи и приема данных, что дает эффективную защиту подключенных к сети приложений. При помощи VPN обеспечивается возможность удаленного подключения к локальной сети, создания общей сети для головного офиса с филиалами. Непосредственно для пользователей VPN дает возможность скрытия местоположения и защиты выполняемых в сети действий.

Прокси-сервер. Выполняет функцию шлюза между компьютером и внешним сервером. Запрос, отправляемый пользователем на сервер, вначале поступает на proxy и уже от его имени поступает на сервер. Возврат ответа производится также с прохождением промежуточного звена — proxy. Преимуществом является то, что кэш прокси-сервера доступен всем пользователем. Это повышает удобство в работе, поскольку наиболее часто запрашиваемые ресурсы находятся в кэше.

Решения SIEM — системы мониторинга и управления информационной безопасностью. Специализированное ПО, которое берет на себя функцию управления безопасностью данных. SIEM обеспечивает сбор сведений о событиях из всех источников, поддерживающих безопасность, в том числе от антивирусного ПО, IPS, файерволов, а также от операционных систем и т. д. На основании анализа данных система выявляет возможные сбои, хакерские атаки, другие отклонения и возможные информационные угрозы.

ИСПЛЬЗОВАННЫЕ ЛИТЕРАТУРЫ:

1. Леонтьев В. Безопсность в сети Интернет.-М:. ОЛМА Медиа Групп, 2008.

2. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам. - М.: ГЛТ, 2016.