# «Информационная безопасность, клептография и криптовирология»

# Информационная безопасность – это сохранение и защита информации, а также её важнейших элементов, в том числе системы и оборудование, которые предназначены для использования, сбережения и передачи этой информации. Другими словами, это набор технологий, стандартов и методов управления, которые необходимы для защиты информационной безопасности (ИБ).

# Цель обеспечения информационной безопасности (ИБ) – это защитить информационные данные и поддерживающую инфраструктуру от случайного или преднамеренного вмешательства, что может стать причиной потери данных или их несанкционированного изменения.

# Роль: специалист по информационной безопасности - Центр оценки и кадрового развития

Информационная безопасность помогает обеспечивать непрерывность бизнеса. Для успешного внедрения систем информационной безопасности на предприятии необходимо придерживаться важных принципов:

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.

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.

Доступность - обеспечивает надежный, а также 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 отрицательным образом.

Принципы корпоративной информационной безопасности возникают на основе корпорации, или организации, члены которой могут быть единым целым. Таким субъектом информационной безопасности может оказаться крупная компания со своими, разработанными в соответствие с потребностями организации, ценностями, холдинговая структура, общественная организация. Главным отличием от обычной структуры информационной безопасности становится повышенная роль персонала или членов корпорации в обеспечении защиты данных.

## Текущие угрозы:

Особенностью корпорации как объединения экономических субъектов становится наличие множества систем и локальных корпоративных сетей разного уровня, для которых необходимо разработать единые регламенты и методики безопасности. Задача требует отвлечения большого объема сил, ресурсов – человеческих, временных, финансовых, и не всегда решается успешно. Только опора на человеческий фактор, создание понимания информационной безопасности как единой ценности компании способны на 70-80 % устранить риски. Но степень угроз растет ежегодно, что требует от специалистов по информационной безопасности особенно высокой квалификации.

Источник угроз сложно определить, если корпорация занимается торговой или производственной деятельностью, не является оператором персональных данных и не владеет объектами ключевой информационной инфраструктуры. Для этих субъектов рынка внешние угрозы всегда более опасны, чем конкуренты. А для корпорации или компании среднего уровня конкуренты более опасны, чем глобальные хакерские группировки. Но наличие сервиса электронных платежей, например, при продаже товаров через интернет сделает их компанией целью для лиц, желающих завладеть не только информацией неопределенной ценности, но и денежными средствами. Основной риск для конфиденциальной информации несет человеческий фактор, уровень защищенности сетей от инсайдеров часто оказывается на низком уровне.

Ключевыми задачами специалиста по информационной безопасности в этих условиях станут:

* Доступность приложений, обеспечивающих бизнес-процессы для пользователей, отсутствие рисков сбоя и выхода из строя системы;
* Доступность интернет-приложений и сайтов с магазинами для клиентов, минимизация риска DDoS-атак.
* Защита ключевой конфиденциальной информации от похищения в результате внешних атак или в результате деятельности инсайдеров. Наиболее уязвимым активом считаются клиентские базы данных, обычно переходящие из компании в компанию вместе с менеджером по продажам.
* Целостность информации, ее сохранность и неизменность в результате внешних вмешательств или работы инсайдеров, желающих внести изменения в данные с целью скрытия неудостоверенных транзакций. Нарушение целостности информации станет проблемой при аудите отчетности, если специалисты проверяющей организации выявят факты вмешательства в структуру данных бухгалтерского или финансового учета.

### Организационные средства:

Организационные средства защиты корпоративной информационной безопасности обычно начинаются с внедрения регламентов и политик, которые, если не поддержаны авторитетом высокого руководства, или молча игнорируются, или, в случае принуждения к их исполнению, вызывают агрессию. Иногда именно такие проявления говорят о том, что конфиденциальные данные находятся под угрозой, кто-то из менеджмента или топовых сотрудников использует их в своих целях и не намерен отказываться от привилегий. Первым шагом на этапе борьбы с этой проблемой становится создание единых этических ценностей, в рамках которых каждый сотрудник корпорации должен ощущать личную ответственность за сохранность данных и соблюдение всех требований регламентов.

Часть компаний по защите данных подталкивают регуляторы, которые выдвигают требования к операторам персональных данных. Несоблюдение требований ФСТЭК и Роскомнадзора к корпоративной информационной безопасности, грозит штрафами либо приостановкой деятельности.

Среди таких требований:

* использование технических средств защиты информации и ПО, прошедшего тестирование и сертификацию и гарантирующего необходимый уровень защиты данных
* соответствие состояния информационной инфраструктуры законам и подзаконным нормативным актам
* разработка стратегии своевременного обновления критичного ПО
* наличие механизма реагирования на инциденты информационной безопасности
* борьба с вирусами с использованием сертифицированных средств антивирусной защиты
* шифрование данных
* принятие пакета документации, регламентирующей все аспекты работ с ИС, обрабатывающими ПД

Но даже для того, чтобы исполнялись требования регуляторов, персонал должен понимать, что при возникновении с его стороны рисков, угрожающих штрафами, денежными потерями в результате исков клиентов, он тоже оказывается в зоне риска с точки зрения выплаты мотивирующих надбавок, сохранения места работы. Необходимо проводить обучение, знакомя сотрудников с моделями рисков и основными способами реакции на них. Необходимость разработки регламентов компании по выполнению требований ИБ создается потребностями модели рисков и работой регуляторов.

Существует раздел криптографии с интересным названием — клептография (kleptography). В нём изучаются методы скрытного ослабления систем шифрования и их использования в нелегальных целях.

Например, для получения конфиденциальных данных, обхода антивирусов, межсетевых экранов и других средств информационной безопасности. Термин «Клептография» был введён в 1996 году Адамом Янгом и Моти Юнгом — известными консультантами по криптографии, работающими на Министерство обороны США и частные компании.

Изначально они называли клептографией внедрение трудно выявляемого бэкдора исключительно в схемы асимметричной криптографии. Такой бэкдор давал возможность вычислить секретный ключ пользователя по его открытому ключу, но только тем, кто знал некий секрет. Как вариант — это был ещё один секретный ключ, общий для бэкдоров одного типа и не зависящий от действий пользователя. Бэкдор - вредоносная программа для получения доступа к рабочей станции, серверу, устройству или сети путем обхода аутентификации, а также других стандартных методов и технологий безопасности.

**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 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 (такие как ITU-T G.hn) защищены с использованием AES для шифрования и X.1035 для аутентификации и обмена ключами.

Клептография стала теоретической основой криптовирологии - методов разработки вредоносного ПО, шифрующего свой код и/или трафик на открытом ключе. К примеру, в последние годы распространились трояны-вымогатели.

Криптовирология - это дисциплина, которая изучает, каким образом можно использовать криптографию разработки и криптоанализа вредоносного программного обеспечения. Понятие криптовирологии зародилось, когда было обнаружено, что шифрование с открытым ключом может использоваться, для создания вредоносного программного обеспечения.

В отличие от предшественников, они уже не просто выполняют на компьютере жертвы шифрование файлов, используя блочный алгоритм (AES, ThreeFish, Serpent). Если бы они этим ограничивались, то вирусный аналитик смог бы проанализировать код трояна и его действия, чтобы найти ключ Ksym - общий для операций шифрования и расшифрования, поскольку все эти алгоритмы симметричные.

Для усложнения атаки современные вирмейкеры прибегают к хитрости: они дополнительно зашифровывают Ksym на открытом ключе (Ko) и отправляют его создателю трояна, после чего удаляют с затиранием свободного места случайными данными. Восстановить Ksym как удалённый файл становится невозможно. Теперь он существует только в зашифрованном виде.

Чтобы расшифровать Ksym, а затем и файлы, аналитику потребуется парный Ko секретный ключ (Ksec), который известен лишь автору трояна, никогда не передавался и не хранился ни на одном заражённом компьютере.

Другой пример из области криптовирологии – это бэкдоры, они крадут конфиденциальную информацию. Они отправляют данные как трафик, зашифрованный открытым ключом. Такой метод широко применяется в легитимных коммуникациях (TLS/ IPSec/ PGP), поэтому не выделяется на общем фоне. При использовании клептографических бэкдоров сложно даже обнаружить факт утечки данных, не говоря уже о попытке выяснить, что и куда передавалось с компьютера жертвы.

Без криптовирологии не появились бы APT (термин кибербезопасности, означающий противника, который обладает современным уровнем специальных знаний и значительными ресурсами, которые позволяют ему создавать угрозу опасных кибератак) - то есть сложные постоянно присутствующие угрозы.

Как правило, часть их компонентов и все взаимодействия с управляющим сервером зашифрованы. Поэтому антивирусы не обнаруживают новые APT до тех пор, пока их действия не станут более явными.

### Заключение:

Информация очень важна для успешного развития бизнесс-процесса и, следовательно, нуждается в соответствующей защите. Особенно актуально в бизнес-среде, где на передний план вышли информационные технологии. Так как мы живем в эпоху цифровой экономики, без них рост компании просто невозможен.

Информация в настоящее время 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 большие обороты. Соответственно возникает необходимость внедрять системы информационной безопасности, которые могли бы защитить данные.

На выбор средств защиты информации влияет достаточно много факторов, включая сферу деятельности компании, ее размер и техническая сторона, а также опыт и знания сотрудников в области информационной безопасности (ИБ).

