Доклад на тему: Информация как ценность. Понятие об информационных угрозах

Основы информационной безопасности

Чувакина Мария Владимировна

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Целью данного доклада является анализ роли информации как ценного ресурса в современном обществе, а также выявление и рассмотрение основных информационных угроз, с которыми сталкиваются организации и индивидуумы. В ходе доклада будет проведено исследование влияния информационных угроз на безопасность данных, репутацию и функционирование организаций, а также предложены рекомендации по минимизации рисков и защите информации в условиях быстро меняющегося цифрового мира.

2 Введение

Стремление зафиксировать, сохранить надолго свое восприятие информации было всегда свойственно человеку. Мозг человека хранит множество информации, и использует для хранения ее свои способы, основа которых – двоичный код, как и у компьютеров. Человек всегда стремился иметь возможность поделиться своей информацией с другими людьми и найти надежные средства для ее передачи и долговременного хранения. Для этого в настоящее время изобретено множество способов хранения информации на внешних (относительно мозга человека) носителях и ее передачи на огромные расстояния.

3 Основные понятия

Угроза информационной безопасности (ИБ) — это возможное негативное воздействие на сеть, программное или аппаратное обеспечение с целью кражи, удаления или порчи информации

4 Информация как ценность

Ценность информации определяется степенью ее полезности для владельца. Обладание истинной (достоверной) информацией дает ее владельцу определенные преимущества. Истинной или достоверной информацией является информация, которая с достаточной для владельца (пользователя) точностью отражает объекты и процессы окружающего мира в определенных временных и пространственных рамках.

Информация, искаженно представляющая действительность (недостоверная информация), может нанести владельцу значительный материальный и моральный ущерб. Если информация искажена умышленно, то ее называют дезинформацией.

Законом «Об информации, информатизации и защите информации» гарантируется право собственника информации на ее использование и защиту от доступа к ней других лиц (организаций). Если доступ к информации ограничивается, то такая информация является конфиденциальной. Конфиденциальная информация может содержать государственную или коммерческую тайну. Коммерческую тайну могут содержать сведения, принадлежащие частному лицу, фирме, корпорации и т. п. Государственную тайну могут содержать сведения, принадлежащие государству (государственному учреждению). В соответствии с законом «О государственной тайне» сведениям, представляющим ценность для государства, может быть присвоена одна из трех возможных степеней секретности. В порядке возрастания ценности (важности) информации ей может быть присвоена степень (гриф) «секретно», «совершенно секретно» или «особой

важности». В государственных учреждениях менее важной информации может присваиваться гриф «для служебного пользования».

Для обозначения ценности конфиденциальной коммерческой информации используются три категории:

- «коммерческая тайна - строго конфиденциально»;
- «коммерческая тайна - конфиденциально»;
- «коммерческая тайна».

Используется и другой подход к градации ценности коммерческой информации:

- «строго конфиденциально - строгий учет»;
- «строго конфиденциально»;
- «конфиденциально».

5 Понятие об информационных угрозах

Угрозы информационной (компьютерной) безопасности — это различные действия, которые могут привести к нарушениям состояния защиты информации. Другими словами, это — потенциально возможные события, процессы или действия, которые могут нанести ущерб информационным и компьютерным системам. Угрозы ИБ можно разделить на два типа: естественные и искусственные. К естественным относятся природные явления, которые не зависят от человека, например ураганы, наводнения, пожары и т.д. Искусственные угрозы зависят непосредственно от человека и могут быть преднамеренными и непреднамеренными. Непреднамеренные угрозы возникают из-за неосторожности, невнимательности и незнания. Примером таких угроз может быть установка программ, не входящих в число необходимых для работы и в дальнейшем нарушающих работу системы, что и приводит к потере информации. Преднамеренные угрозы, в отличие от предыдущих, создаются специально. К ним можно отнести атаки злоумышленников как извне, так и изнутри компании. Результат реализации этого вида угроз — потери денежных средств и интеллектуальной собственности организации.

6 Классификация угроз информационной безопасности

В зависимости от различных способов классификации все возможные угрозы информационной безопасности можно разделить на следующие основные подгруппы:

- Нежелательный контент
- Несанкционированный доступ
- Утечки информации
- Потеря данных
- Мошенничество
- Кибервойны
- Кибертерроризм

Нежелательный контент — это не только вредоносный код, потенциально опасные программы и спам (т.е. то, что непосредственно создано для уничтожения или кражи информации), но и сайты, запрещенные законодательством, а также нежелательные ресурсы с информацией, не соответствующей возрасту потребителя.

Несанкционированный доступ — просмотр информации сотрудником, который не имеет разрешения пользоваться ею, путем превышения должностных полномочий. Несанкционированный доступ приводит к утечке информации. В зависимости от того, каковы данные и где они хранятся, утечки могут организо-

вываться разными способами, а именно через атаки на сайты, взлом программ, перехват данных по сети, использование несанкционированных программ.

Утечки информации можно разделять на умышленные и случайные. Случайные утечки происходят из-за ошибок оборудования, программного обеспечения и персонала. Умышленные, в свою очередь, организовываются преднамеренно с целью получить доступ к данным, нанести ущерб.

Потерю данных можно считать одной из основных угроз информационной безопасности. Нарушение целостности информации может быть вызвано неисправностью оборудования или умышленными действиями людей, будь то сотрудники или злоумышленники.

Не менее опасной угрозой является мошенничество с использованием информационных технологий («фрод»). К мошенничеству можно отнести не только манипуляции с кредитными картами («кардинг») и взлом онлайн-банка, но и внутренний фрод. Целями этих экономических преступлений являются обход законодательства, политики безопасности или нормативных актов, присвоение имущества.

Ежегодно по всему миру возрастает террористическая угроза, постепенно перемещаясь при этом в виртуальное пространство. На сегодняшний день никого не удивляет возможность атак на автоматизированные системы управления технологическими процессами (АСУ ТП) различных предприятий. Но подобные атаки не проводятся без предварительной разведки, для чего применяется кибершпионаж, помогающий собрать необходимые данные. Существует также такое понятие, как «информационная война»; она отличается от обычной войны тем, что в качестве оружия выступает тщательно подготовленная информация.

7 Источник угроз информационной безопасности

Нарушение режима информационной безопасности может быть вызвано как спланированными операциями злоумышленников, так и неопытностью сотрудников. Пользователь должен иметь хоть какое-то понятие об ИБ, вредоносном программном обеспечении, чтобы своими действиями не нанести ущерб компании и самому себе. Такие инциденты, как потеря или утечка информации, могут также быть обусловлены целенаправленными действиями сотрудников компании, которые заинтересованы в получении прибыли в обмен на ценные данные организации, в которой работают или работали.

Основными источниками угроз являются отдельные злоумышленники («хакеры»), киберпреступные группы и государственные спецслужбы (киберподразделения), которые применяют весь арсенал доступных киберсредств, перечисленных и описанных выше. Чтобы пробиться через защиту и получить доступ к нужной информации, они используют слабые места и ошибки в работе программного обеспечения и веб-приложений, изъяны в конфигурациях сетевых экранов и настройках прав доступа, прибегают к прослушиванию каналов связи и использованию клавиатурных шпионов.

То, чем будет производиться атака, зависит от типа информации, ее расположения, способов доступа к ней и уровня защиты. Если атака будет рассчитана на неопытность жертвы, то возможно, например, использование спам-рассылок.

Оценивать угрозы информационной безопасности необходимо комплексно,

при этом методы оценки будут различаться в каждом конкретном случае. Так, чтобы исключить потерю данных из-за неисправности оборудования, нужно использовать качественные комплектующие, проводить регулярное техническое обслуживание, устанавливать стабилизаторы напряжения. Далее следует устанавливать и регулярно обновлять программное обеспечение (ПО). Отдельное внимание нужно уделить защитному ПО, базы которого должны обновляться ежедневно.

Обучение сотрудников компании основным понятиям информационной безопасности и принципам работы различных вредоносных программ поможет избежать случайных утечек данных, исключить случайную установку потенциально опасного программного обеспечения на компьютер. Также в качестве меры предосторожности от потери информации следует делать резервные копии. Для того чтобы следить за деятельностью сотрудников на рабочих местах и иметь возможность обнаружить злоумышленника, следует использовать DLP-системы.

Организовать информационную безопасность помогут специализированные программы, разработанные на основе современных технологий: - защита от нежелательного контента (антивирус, антиспам, веб-фильтры, анти-шпионы); - сетевые экраны и системы обнаружения вторжений (IPS); - управление учетными данными (IDM); - контроль привилегированных пользователей (PUM); - защита от DDoS; - защита веб-приложений (WAF); - анализ исходного кода; - антифрод; - защита от таргетированных атак; - управление событиями безопасности (SIEM); - системы обнаружения аномального поведения пользователей (UEBA); - защита АСУ ТП; - защита от утечек данных (DLP); - шифрование; - защита мобильных устройств; - резервное копирование; - системы отказоустойчивости.

8 Вывод

В современном обществе информация является одним из самых ценных ресурсов, и ее защита становится приоритетной задачей как для организаций, так и для индивидуумов. Угрозы информационной безопасности, как естественные, так и искусственные, могут привести к серьезным последствиям, включая утечку данных, финансовые потери и ущерб репутации. Важно понимать, что источниками угроз могут быть как внешние злоумышленники, так и внутренние факторы, такие как неосторожность сотрудников.

Для эффективной защиты информации необходимо применять комплексный подход, который включает в себя как технические меры, так и обучение персонала. Использование современных технологий и программного обеспечения, таких как антивирусы, системы обнаружения вторжений и DLP-системы, позволяет минимизировать риски и повысить уровень безопасности данных.

Кроме того, регулярное обновление программного обеспечения, создание резервных копий и внедрение политики безопасности помогут предотвратить инциденты, связанные с потерей или утечкой информации. В конечном итоге, осознание ценности информации и активные меры по ее защите являются ключевыми факторами для успешного функционирования организаций в условиях быстро меняющегося цифрового мира.