Доклад по теме
Информация как ценность. Понятие об информационных угрозах.

Информационная безопасность

Выполнила: Коняева Марина Александровна,
НФИбд-01-21, 1032217044

Содержание

Список иллюстраций

Введение

На сегодняшний день информация является одним из наиболее ценных и весомых продуктов человеческой деятельности. Эффективность работы организации в значительной степени зависит от наличия соответствующей информации, методологии ее использования и концепции защиты информационной системы. Одним из основных аспектов проблемы обеспечения безопасности является определение,анализ и классификация возможных угроз. Перечень наиболее значимых угроз,оценка их вероятности и модель злоумышленника являются базовой информацией для построения оптимальной системы защиты.

Угрозы информационной 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 .

Классификация угроз информационной безопасности

Угрозы ИБ можно разделить на два типа по природе возникновения: естественные и искусственные. К естественным относятся природные явления, которые не зависят от человека, например ураганы, наводнения, пожары и т.д.

По степени преднамеренности: 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.

По положению: внутренние (например, перехват данных, передаваемых по сети или утечка) и внешние (хищение носителей с конфиденциальной информацией)

По степени воздействия: пассивные (угрозы, не нарушающие состав и нормальную работу) и активные (которые нарушаютнормальное функционирование системы, ее структуру или состав)

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

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

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

Утечки информации

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 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 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 .

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, 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 .

Методы обеспечения защиты информации

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.

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; управление учетными данными; контроль привилегированных

пользователей; защита веб-приложений; анализ исходного кода; антифрод ; защита от таргетированных атак; управление событиями безопасности; системы обнаружения аномального поведения пользователей; защита АСУ ТП; защита от утечек данных; шифрование ; защита мобильных устройств; резервное копирование; системы отказоустойчивости
.

Заключение

Информация представляет собой ценность, определяющую успех в различных сферах деятельности, и с ростом значимости информации возрастают и информационные угрозы, способные нанести серьезный ущерб личности, бизнесу и обществу в целом.

Обеспечение информационной безопасности становится крайне важным заданием в настоящее время, применяя комплексный подход, ряд методов и средств для защиты информации.

Список литературы. Библиография

[1] Основы информационной безопасности: учебно-практическое пособие / ю.н. Сычев. М.: ИЗД. ЦентЕДОИ, 2010. - 328 сн

[2] Информационная безопасность вычислительной техники : учебное пособие / В.Г. Спицын. - Томск: Эль Контент, 2011. - 148 с.3.

[3] Основы информационной безопасности : учеб. Пособие / С.А. Нестеров. - СПб.: Изд-во Политехн. ун-та, 2014. — 322 с.

[4] Информационная безопасность и защита информации: учебник / О.В. Прохорова. — Самара: СГАСУ, 2006. — 264 с.

[5] Информационная безопасность (2-я книга социально-политического проекта «Актуальные проблемы безопасности социума»). // «Оружие и технологии», № 11, 2014 - С.15-21.