Система ИБ. Объекты защиты. Категории и носители информации. Средства защиты информации. Обеспечение защиты.

Выполнили: Осипов Руслан, Евгений Хлыбов

Система ИБ

Система информационной безопасности для компании – юридического лица включает три группы основных понятий: целостность, доступность и конфиденциальность. Под каждым скрываются концепции с множеством характеристик.

Под **целостностью** понимается устойчивость баз данных, иных информационных массивов к случайному или намеренному разрушению, внесению несанкционированных изменений. Понятие целостности может рассматриваться как:

- **статическое**, выражающееся в неизменности, аутентичности информационных объектов тем объектам, которые создавались по конкретному техническому заданию и содержат объемы информации, необходимые пользователям для основной деятельности, в нужной комплектации и последовательности;
- **динамическое**, подразумевающее корректное выполнение сложных действий или транзакций, не причиняющее вреда сохранности информации.

Для контроля динамической целостности используют специальные технические средства, которые анализируют поток информации, например, финансовые, и выявляют случаи кражи, дублирования, перенаправления, изменения порядка сообщений. Целостность в качестве основной характеристики требуется тогда, когда на основе поступающей или имеющейся информации принимаются решения о совершении действий. Нарушение порядка расположения команд или последовательности действий может нанести большой ущерб в случае описания технологических процессов, программных кодов и в других аналогичных ситуациях.

- **Доступность** – это свойство, которое позволяет осуществлять доступ авторизированных субъектов к данным, представляющим для них интерес, или обмениваться этими данными. Ключевое требование легитимации или авторизации субъектов дает возможность создавать разные уровни доступа. Отказ системы предоставлять информацию становится проблемой для любой организации или групп пользователей. В качестве примера можно привести недоступность сайтов госуслуг в случае системного сбоя, что лишает множество пользователей возможности получить необходимые услуги или сведения.
- **Конфиденциальность** означает свойство информации быть доступной тем пользователям: субъектам и процессам, которым допуск разрешен изначально. Большинство компаний и организаций воспринимают конфиденциальность как ключевой элемент ИБ, однако на практике реализовать ее в полной мере трудно. Не все данные о существующих каналах утечки сведений доступны авторам концепций ИБ, и многие технические средства защиты, в том числе криптографические, нельзя приобрести свободно, в ряде случаев оборот ограничен.
- Равные свойства ИБ имеют разную ценность для пользователей, отсюда – две крайние категории при разработке концепций защиты данных. Для компаний или организаций, связанных с государственной тайной, ключевым параметром станет конфиденциальность, для публичных сервисов или образовательных учреждений наиболее важный параметр – доступность.

Объекты защиты в концепциях ИБ

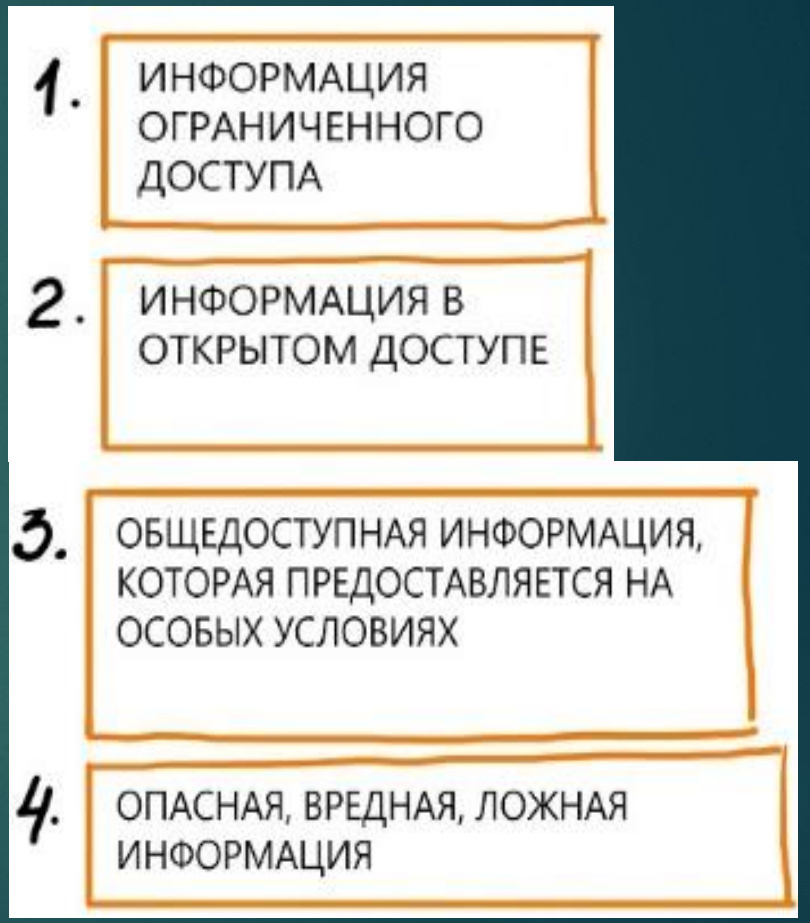
Различие в субъектах порождает различия в объектах защиты. Основные группы объектов защиты:

- информационные ресурсы всех видов (под ресурсом понимается материальный объект: жесткий диск, иной носитель, документ с данными и реквизитами, которые помогают его идентифицировать и отнести к определенной группе субъектов);
- права граждан, организаций и государства на доступ к информации, возможность получить ее в рамках закона; доступ может быть ограничен только нормативно-правовыми актами, недопустима организация любых барьеров, нарушающих права человека;
- система создания, использования и распространения данных (системы и технологии, архивы, библиотеки, нормативные документы);
- система формирования общественного сознания (СМИ, интернет-ресурсы, социальные институты, образовательные учреждения).

Каждый объект предполагает особую систему мер защиты от угроз ИБ и общественному порядку. Обеспечение информационной безопасности в каждом случае должно базироваться на системном подходе, учитывающем специфику объекта.

Категории и носители информации

- информация, доступ к которой ограничен на основании требований законов (государственная тайна, коммерческая тайна, персональные данные);
- сведения в открытом доступе;
- общедоступная информация, которая предоставляется на определенных условиях: платная информация или данные, для пользования которыми требуется оформить допуск, например, библиотечный билет;
- опасная, вредная, ложная и иные типы информации, оборот и распространение которой ограничены или требованиями законов, или корпоративными стандартами.



Средства защиты информации

Для целей разработки концепций ИБ-защиты средства защиты информации принято делить на нормативные (неформальные) и технические (формальные).

Неформальные средства защиты – это документы, правила, мероприятия, **формальные** – это специальные технические средства и программное обеспечение. Разграничение помогает распределить зоны ответственности при создании ИБ-систем: при общем руководстве защитой административный персонал реализует нормативные способы, а IT-специалисты, соответственно, технические.

Основы информационной безопасности предполагают разграничение полномочий не только в части использования информации, но и в части работы с ее охраной. Подобное разграничение полномочий требует и нескольких уровней контроля.

Построение системы защиты персональных данных

Классификация уровней защиты

Информационная безопасность подразумевает четыре уровня защиты от угроз:

- Первый уровень. Наиболее высокий, предполагает полную защиту специальных персональных данных (национальная и расовая принадлежность, отношение к религии, состояние здоровья и личная жизнь).
- Второй уровень. Предполагает защиту биометрических данных (в том числе фотографии, отпечатки пальцев).
- Третий уровень. Представляет собой защиту общедоступных данных, то есть тех, к которым полный и неограниченный доступ предоставлен самим человеком.
- Четвертый уровень. Это сборная группа, в которую включают все данные, не упомянутые в предыдущих трех пунктах.

Таким образом, все данные, собранные в информационной базе компании, могут быть четко распределены по уровням защиты.

Обеспечение защиты

Защита информации по уровням в каждом случае состоит из цепочки мер.

- Четвертый уровень. Означает исключение из помещения, где находится информационное оборудование, посторонних лиц, обеспечение сохранности носителей данных, утверждение четкого списка работников, которые имеют допуск к обработке данных, а также использование специальных средств защиты информации.
- Третий уровень. Подразумевает выполнение всех требований, предусмотренных для предыдущего уровня, и назначение ответственного за информационную безопасность должностного лица.
- Второй уровень. Помимо выполнения требований предыдущего уровня, включает в себя ограничение доступа к электронному журналу безопасности.
- Первый уровень. Кроме всех требований, которым необходимо следовать на втором уровне, включает обеспечение автоматической регистрации в электронном журнале безопасности полномочий сотрудников, имеющих доступ к данным, в случае изменения этих полномочий, а также возложение ответственности за информационную безопасность на специально созданное подразделение.

Должное выполнение прописанных в законодательстве мер защиты персональных данных в соответствии с уровнями обеспечивает максимальную эффективность общей стратегии защиты информации, принятой в компании.

Источники:

- https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/

- https://www.smart-soft.ru/blog/praktika-sozdanie-sistemy-zaschity-personaljnyh-dannyh/