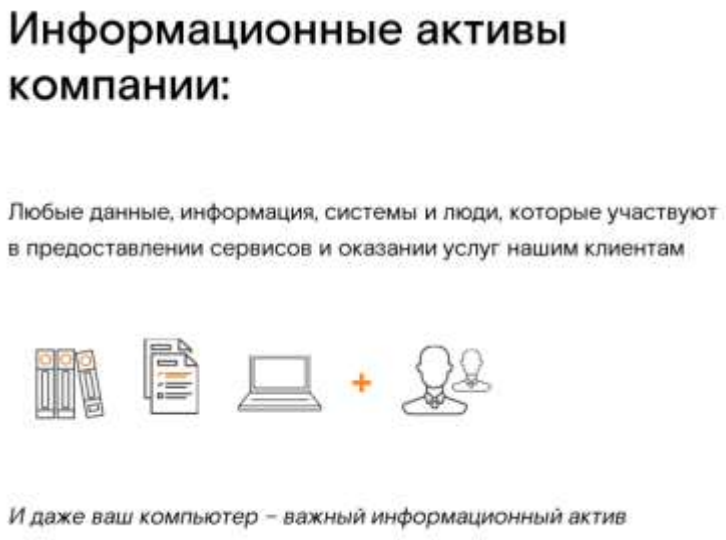
Общие вопросы информационной безопасности

что такое информационные активы,
классификация информационных активов,
почему важна безопасность
какие существуют угрозы,
как работать и оставаться в безопасности
как защитить личные данные и данные клиентов.

Классификация информационных активов (ИА) это важнейший процесс не только для обеспечения ИБ, но так же и построения управляемой ИТ-инфраструктуры всей компании. Классификация позволяет получить ключевые метрики для используемой информации - ценность, степень влияния на бизнес-процессы, требования к обеспечению т.д. От качества выполненной классификации во многом зависит то как будет защищаться и обрабатываться информация. Более того, многие нормативные стандарты требует проведения обязательной инвентаризации и классификации ИА. Однако, какой либо единой процедуры на этот счет не существует. В сегодняшнем материалы мы попытаемся систематизировать имеющийся опыт по методике классификации ИА, а так же рассмотрим общие подходы существующие на сегодняшний день



Если, вспомнить определения, приведенные в отраслевом стандарте Банка России СТО БР ИББС-1.0-2014, то там четко прописаны определения:

- **Информационный актив** - Информация с реквизитами, позволяющими ее идентифицировать; имеющая ценность для организации БС РФ; находящаяся в распоряжении организации БС РФ и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме.
- **Классификация информационных активов** - Разделение существующих информационных активов организации БС РФ по типам, выполняемое в соответствии со степенью тяжести последствий от потери их значимых свойств ИБ.

Так же термин классификация упоминается в ряде отечественных и международных стандартах, например:

ISO/IEC TR 13569:2005 Финансовые услуги – Рекомендации по информационной безопасности

Классификация – это схема, разделяющая информацию на категории, такие как: возможность мошенничества, конфиденциальность или критичность информации, с целью возможности применения соответствующих защитных мер

Р Газпром 4.2.3-001. Методика классификации объектов защиты

Классификация объектов защиты выполняется с целью обеспечения дифференцированного подхода к организации их защиты с учетом уровня критичности, характеризующего влияние на деятельность и репутацию организации, ее деловых партнеров, клиентов и работников

Классификация позволяет определить приоритетность и экономическую целесообразность проведения дальнейших мероприятий по обеспечению информационной безопасности объекта защиты

Другие документы в которых так же есть отсылка к классификации ИА:

- ISO/IEC 27002:2005 Информационные технологии – Свод правил по управлению защитой информации
- ISO/IEC 20000-2 Информационные технологии – Управление услугами. Свод практик

Более того в Российской Федерации для обеспечения защиты конфиденциальной информации в режиме коммерческой тайны (КТ) согласно ФЗ от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне», собственнику просто необходимо произвести классификацию имеющихся у него ИА.

Для проведения классификации ИА в соответствии с нормами действующего законодательства РФ определены следующие типы информации:

- открытая (общедоступная) информация;
- персональные данные (ПДн) ;
- информация, содержащая сведения, составляющие банковскую тайну (БТ), согласно федеральному закону , в том числе неплатежная информация;
- информация, содержащая сведения, составляющие коммерческую тайну (КТ)

Классификацию ИА можно выполнять основываясь по одной из следующих моделей:

1. Однофакторная классификация основанная на степени ущерба.
По сути здесь все просто, классифицируем информацию, к примеру на четыре блока по степени нанесения ущерба в случае ее утечки - минимальный, средний, высокий и критический. Так, например, если неопределенному кругу лиц станет известно о том, кого сегодня директор принимает в своем кабинете это один вид ущерба (минимальный), другое дело если утекут условия и детали сделки по какому-либо крупному проекту (высокий или критический)

2. Многофакторная модель классификации по трем классическим параметрам
Здесь вся информация рассматривается с точки зрения обеспечения ее конфиденциальности, целостности и доступности. И так для каждого отдельного ИА проставляется требования отдельно по трем описанным позициям - высокий, средний, низкий. По совокупности так можно будет качественно оценить ИА, к примеру, критичной важности или базовой важности.

Для перехода к количественной оценке информационных активов необходимо ввести классы, отражающие как ценность ИА, так и уровень требований к защите ИА.

Каждому ИА в таком случае будет присвоен соответствующий класс:

- ***Открытый (О)*** – ограничения на распространение и использование не накладываются, финансовый ущерб отсутствует;

- ***Для служебного использования (ДСП)*** – для использования внутри организации, финансовый ущерб отсутствует, возможно возникновения иных видов ущерба для организации или работников организации;
- ***Конфиденциальная (КТ)*** – для использования как внутри организации так и при обмене с клиентами и контрагентами, финансовый ущерб реален

В свою очередь ***Конфиденциальную информацию (КТ)*** можно условно разделить на несколько подкатегорий для градации по степени ценности:

- С ограниченным доступом (Д) – для использования определенным кругом работников организации, финансовый ущерб, к примеру до 1 млн. рублей;
- Секретный (С) – для использования только определенными членами руководящего состава организации, финансовый ущерб, к примеру, более 1 млн. рублей.

В итоге мы можем получить следующую таблицу

Реестр информационных активов

№	Название группы информационных активов	Описание	Формат	Размещение		Класс	Тип	Требования к конф-ти	Требования к цел-ти	Требования к дост-ти	Владелец	Пользователь
				Физ. р.	ИС/прил./хран							
1.	Лицензии на программное обеспечение (ПО)	Документы, содержащие сведения о праве использования ПО	Б/Э	Отдел ИБ	Департамент ИТ	Д	Не установлен	Средние	Высокие	Средние	Главный бухгалтер	ДИТ
2.	Дистрибутивы с ПО	Носители, содержащие установочные комплекты (дистрибутивы) ПО	Э	Департамент ИТ	Департамент ИТ	ВИ	Не установлен	Низкие	Средние	Средние	Начальник ДИТ, Начальник ОИБ	ДИТ, ОИБ
3.												

Независимо от характера самих информационных ресурсов, они обязательно обладают одной или несколькими из следующих характеристик:

- Они признаются ценными для организации.
- Их невозможно заменить без затрат средств, времени, иных ресурсов или их сочетания.
- Они существенно влияют на деятельность организации, без этих ресурсов возникает угроза для основной деятельности организации.

В целом схема выполенеия классифиакции ИА может быть следующей:

Этап 1. Построение перечня ИА и схемы ИА

На данном этапе необходимо выявить ИА в любом виде (электронные документы, бумажные документы, флешки, информационный потоки и т.п.) циркулирующие между подразделениями в вашей организации, не углубляясь в документооборот внутри подразделений.
Для этого в подразделения рассылается анкета с полями вида:

Какую информацию, в каком виде и от каких подразделений вы получаете?
Какую информацию, в каком виде и в какие подразделения вы передаете?

После этого собираете данные от подразделений, уточняете её и на основе этого строите большую схему, показывающую циркуляцию информации.

В итоге на выходе получаются следующие документы:
1. Перечень ИА
2. Схема ИА

Этап 2. Построение перечня ИА и схемы ИА на уровне подразделений,
Работа та же самая, что и на 1м этапе, но уже рассматриваем каждое подразделение отдельно.

Этап 3. Начинаем привязывать ИА к инфраструктуре, где хранятся, по каким каналам передаются, в каких информационных системах содержатся и тд.

Тут уже берем один ИА и рисуем всю его среду обитания (чем подробнее, тем лучше, тк. потом будет проще выявлять угрозы. Т.е. пишем порты передачи, по каким каналам итд, думаю вам, как ИТшнику это будет проще всего).

Этап 4. Берем все, что наработали и повторно классифицируем (для окончательной ясности) ИА по характеристикам (К,Ц,Д).

Примерная модель классификации (буквено-цифровое кодирование)

Таким образом можно предложить следующую модель для классификации информационных объектов. Для удобства дальнейших ссылок на класс категории рекомендуем сразу ввести буквенно-цифровое обозначение (в приведенном примере литера "Д" означает "доступность", "Ц" — "целостность"* "К" — "конфиденциальность", цифры возрастают с убыванием значимости критерия).

По наличию (доступность)

- Критическая — без нее работа субъекта останавливается (ДО).
- Очень важная — без нее можно работать, но очень короткое время (Д1).
- Важная — без нее можно работать некоторое время, но рано или поздно она понадобится (Д2)
- Полезная — без нее можно работать, но ее использование экономит ресурсы (Д3).
- Несущественная — устаревшая или неиспользуемая, не влияющая на работу субъекта (Д4).
- Вредная — ее наличие требует обработки, а обработка ведет к расходу ресурсов, не давая результатов либо принося ущерб (Д5). (В определенных организациях может понадобиться и такой параметр.)

По несанкционированной модификации (целостность)

- Критическая — ее несанкционированное изменение приведет к неправильной работе всего субъекта или значительной его части; последствия модификации необратимы (ЦО)

- Очень важная — ее несанкционированное изменение приведет к неправильной работе субъекта через некоторое время, если не будут предприняты некоторые действия; последствия модификации необратимы (Ц1).
- Важная — ее несанкционированное изменение приведет к неправильной работе части субъекта через некоторое время, если не будут предприняты некоторые действия; последствия модификации обратимы (Ц2).
- Значимая — ее несанкционированное изменение скажется через некоторое время, но не приведет к сбою в работе субъекта; последствия модификации обратимы (Ц3).
- Незначимая — ее несанкционированное изменение не скажется на работе системы (Ц4).

По разглашению (конфиденциальность)

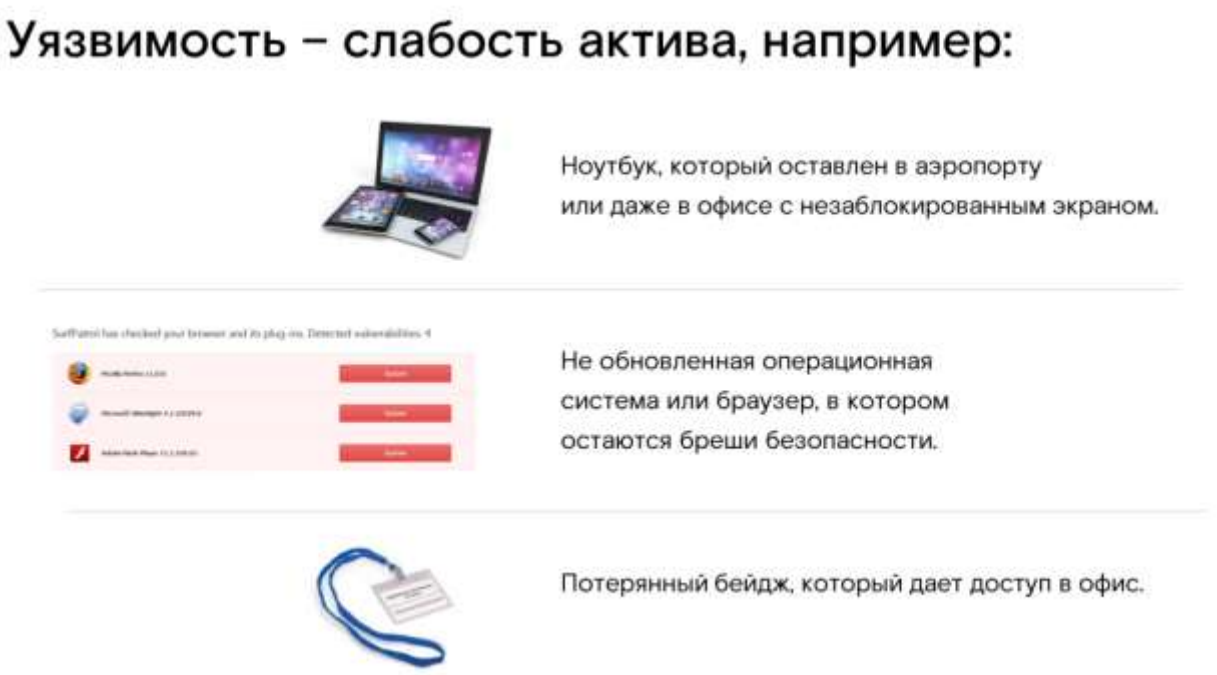
- Критическая — разглашение информации приведет к краху работы субъекта или к очень значительным материальным потерям (К0).
- Очень важная — разглашение приведет к значительным материальным потерям, если не будут предприняты некоторые действия (К1).
- Важная — разглашение приведет к некоторым материальным (может быть, косвенным) или моральным потерям, если не будут предприняты некоторые действия (К2).
- Значимая — приносит скорее моральный ущерб, может быть использована только в определенных ситуациях (К3).
- Малозначимая — может принести моральный ущерб в очень редких случаях (К4).
- Незначимая — не влияет на работу субъекта (К5).

Каждая из указанных выше категорий информации имеет свой жизненный цикл, по истечении периодов которого степень важности объекта, как правило, **снижается**.

Жизненный цикл обычно можно обозначить следующими стадиями.

- Информация используется в операционном режиме, т. е. принимает участие в производственном цикле и бывает востребована практически постоянно.
- Информация используется в архивном режиме, т. е. не принимает непосредственного участия в производственном цикле, но периодически требуется для аналитической или другой деятельности.
- Информация хранится в архивном режиме для обеспечения соответствия требованиям сохранения (например, вышестоящей организации), практически не нужна самому предприятию.

Уязвимости и угрозы безопасности



Угрозы информационной безопасности – комбинация действий, факторов, внешних условий, формирующих вероятность нарушения ИБ конкретной системы. Под угрозой принято понимать события или действия, способные нанести вред и ущерб потребностям, возможностям, имуществу человека или организации.
Основными принципами информационной безопасности являются:

- Целостность. Свойство данных по сохранению своего первоначального вида вне зависимости от длительности хранения и количества передач.
- Конфиденциальность. Ограничение доступа к конкретным сведениям, доступным только для узкого кругла лиц.
- Доступность. Данные, находящиеся в свободном доступе, должны быть предоставлены всем заинтересованным лицам вовремя, без ограничений.
- Достоверность. Сохранение авторства созданных и опубликованных данных за определенным лицом, выступающем в качестве источника сведений.

Классификация угроз информационной безопасности

Принято выделять категории угроз ИБ, которые классифицируются по разным признакам:

- по части системы информационной безопасности, в отношении которой идут угрозы (конфиденциальности, целостности, доступности).
- по местонахождению источника (наружные, внутренние);
- по объему предполагаемого нанесенного ущерба (общий, локальный, частный);
- по уровню воздействия на ИБ (пассивные, активные);
- по характеру появления (естественные, искусственные/объективные, субъективные).
-

В качестве угрозы ИБ понимается потенциально вероятное событие или действие, которое способно нанести системе ущерб. Экспертами в сфере информационной безопасности насчитывается около 100 различных видов угроз ИБ, поэтому ИБ-специалисты во время своей профессиональной деятельности должны анализировать все риски с использованием различных диагностических методик для формирования эффективной защитной системы от потенциальных угроз.

Наиболее частыми угрозами, которые сейчас встречаются в мировом информационном пространстве, являются:

- Нежелательный контент. Вредоносное ПО, опасный софт, ненужный спам, веб-ресурсы, которые запрещены законами страны, нежелательные порталы с данными, которые не соответствуют возрасту или типу потребителя контента.
- Несанкционированный доступ. Просмотр и использование в определенных целях информации лицами, которые не имеют к ней разрешенной доступа. Несанкционированный доступ становится причиной утечки данных. Организация утечек может происходит различными методами: кибератаки на сайты, взлом приложений, перехват трафика, применение вредоносного ПО и т. д.
- Потеря данных. Одна из главный угроз ИБ. Целостность информации нарушается при неисправности используемого оборудования, при преднамеренных действиях сотрудников компании или третьих лиц.

Классификация уязвимостей систем безопасности

Угрозы в отношении ИБ конкретной системы или сети появляются в результате взаимодействия с самыми ненадежными частями созданной защиты – через факторы уязвимости. Большая часть известных уязвимостей появляются из-за действия определенных факторов:

- недостаточное качество используемого ПО, аппаратной платформы;
- непростые эксплуатационные условия, неграмотное размещение информационных данных;
- низкая точность протоколов обмена данными и интерфейса;
- различные параметры архитектуры автоматизированных систем в инфопотоках;
- неполноценные процессы, функционирующие в системе.

Запуск источников угроз со стороны злоумышленников происходит для получения неправомерной выгоды за счет нанесению ущербу информационным данным.

Уязвимости принято делить на три основных класса:

- объективные (зависят от техноснащения на объекте, который нуждается в защите, от настроек и характеристик используемого оборудования);
- случайные (возникают на фоне форс-мажорных обстоятельств, специфики инфосреды, которая окружает объект);
- субъективные (формируются из-за неграмотных действий специалистов во время создания систем хранения/защиты данных).

Источники, угрожающие информационной безопасности

Также требуется классифицировать источники, которые угрожают информационной безопасности объекта. Принято выделять следующие критерии:

1. По типу намеренности осуществления вмешательства в систему защиты: случайное вмешательство со стороны сотрудников компании и намеренное вмешательство со стороны киберпреступников для получения личных выгод.
2. По природе возникновения: угрозы, спровоцированные действиями человека (искусственные) и угрозы, которые не могут быть проконтролированы информационным системам (к примеру, ставшие следствием стихийных бедствий).
3. По причине возникновения. В качестве виновника могут выступать:

- люди, разглашающие конфиденциальные данные с применением подкупа ответственных лиц;

- природные факторы, ставшие причиной аварии, катастрофы, возникновения различных нарушений в функционале оборудования;
- интеграция вредоносного кода или использование неподходящего ПО, нарушающего работу системы;
- непреднамеренное удаление информации, отказ в работе ОС и т. п.

4. По активности воздействия угроз на инфоресурсы (при обработке информации, при передаче данных, вне зависимости от типа работы системы в данный момент).

В организации защиты информации, конфиденциальных данных помогают специализированные программы, программное обеспечение, приложения, инструменты. К таковым относятся: антивирусное ПО, web-фильтры, IDM, IPS, PUM, защита от DDoS-атак, систематический анализ исходного кода, анализ web-приложений, управление событиями безопасности, защита АСУ ТП, шифрование, защита мобильных устройств и мобильных приложений, резервное копирование и другие решения.

Как работать и оставаться в безопасности защитить личные данные и данные клиентов

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.

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.

Не допускайте посторонних

Носите бейдж, если он у вас есть.

Обращайте внимание на людей без бейджа и сопровождения. Проводите их на ресепшен или к охране.

Не оставляйте после себя открытую дверь – никто не должен пройти за вами без пропуска.

Соблюдайте порядок на рабочем месте

Держите свой стол в чистоте, не оставляйте документы и любые бумаги на столе после рабочего дня.

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

Подробный список технических и организационных мер по обеспечению безопасности также определен юридически. К ним относятся процедура идентификации и аутентификации субъектов и объектов доступа, цепочка управления доступом, ограничение программной среды, надежная защита машинных носителей информации, антивирусная защита, предотвращение и обнаружение вторжений, аналитика степени защищенности среды наряду с обеспечением доступности данных и выявлением событий, которые потенциально приведут к сбоям в работе системы. Кроме того, закон обязывает в случае технической невозможности реализации каких-либо мер разрабатывать другие, компенсирующие меры по нейтрализации угроз.

Не подключайте неизвестные флешки

- Не подключайте неизвестные флешки и другие USB-устройства к рабочему компьютеру
- Даже если вы нашли их в офисе или на своем столе
- Даже если кто-то прислал их вам по почте
- Даже если они выглядят так мило

Каждая флешка может содержать вредоносную программу BadUSB

USB-устройство может уничтожить ваш компьютер USB Killer

Технические средства защиты также имеют отдельную классификацию и должны выбираться в зависимости от требуемого уровня защиты. Средства определены официальным документом, составленным Федеральной службой по техническому и экспортному контролю (орган исполнительной власти, занимающийся защитой информации). Документ доступен на официальном ресурсе службы. Каждый из классов имеет минимальный набор требований по защите.

Сохраняйте пароль в тайне

Ваша учетная запись – ваша собственность, и только вы знаете пароль от нее и отвечаете за все действия.

Не говорите и не высылайте свой пароль никогда и НИКОМУ, даже сотруднику ИТ.

Криптографические средства защиты информации

Одним из наиболее действенных способов защиты персональных данных является использование средств криптографии. Если упростить, то речь идет о шифровании текста с помощью цифрового кода.

К криптографическим средствам относятся аппаратные, программные и комбинированные устройства и комплексы, способные реализовывать алгоритмы криптографического преобразования информации.

Они предназначены одновременно для защиты информации при передаче по каналам связи и защиты ее от неразрешенного доступа при обработке и хранении. Логика проста: злоумышленник, который не знает кода, не сможет воспользоваться данными, даже если получит к ним доступ, поскольку не прочтет их. Для него они останутся бессмысленным набором как будто случайных цифр.

Регламент использования криптографических средств определяется Федеральной службой безопасности и документирован в соответствующем приказе.