**Лекция 2:**

**Виды угроз информационной безопасности**

**Аннотация:**В лекции приводятся виды угроз информационной безопасности, классификация источников угроз и защищаемой информации.

**Виды угроз информационной безопасности и классификация источников угроз**

Угрозы возникают из противоречий экономических интересов различных элементов, взаимодействующих как внутри, так и вне социально-экономической системы — в том числе и в информационной сфере. Они и определяют содержание и направления деятельности *по* обеспечению общей и информационной безопасности. Следует отметить, что *анализ* проблем экономической безопасности необходимо проводить, учитывая взаимосвязи экономических противоречий, угроз и потерь, к которым может приводить реализация угроз. Такой *анализ* приводит к следующей цепочке:

<*источник угрозы* (внешняя и/или внутренняя среда предприятия)>

<зона риска (сфера экономической деятельности предприятия, способы её реализации, материальные и информационные ресурсы)>

<фактор (степень уязвимости данных, информации, программного обеспечения, компьютерных и телекоммуникационных устройств, материальных и финансовых ресурсов, персонала)>

<*угроза* (вид, величина, направление)>

<возможность её реализации (предпосылки, *объект*, способ действия, скорость и временной *интервал* действия)>

<последствия (материальный *ущерб*, моральный вред, *размер ущерба* и вреда, возможность компенсации)>.

Угрозу отождествляют обычно либо с характером (видом, способом) дестабилизирующего воздействия на материальные объекты, *программные средства* или информацию, либо с последствиями (результатами) такого воздействия.

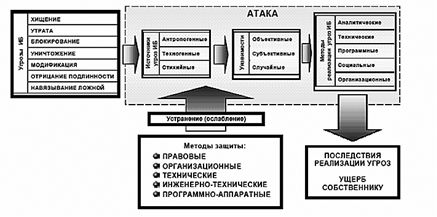
С правовой точки зрения понятие *угроза* жестко связано с юридической категорией *ущерб*, которую Гражданский Кодекс РФ (часть I, ст. 15) определяет как "фактические *расходы*, понесенные субъектом в результате нарушения его прав (например, кражи, разглашения или использования нарушителем конфиденциальной информации), утраты или повреждения имущества, а также *расходы*, которые он должен будет произвести для восстановления нарушенного *права* и стоимости поврежденного или утраченного имущества".

*Анализ* негативных последствий возникновения и осуществления угроз предполагает обязательную идентификацию возможных источников угроз, уязвимостей, способствующих их проявлению и методов реализации. В связи с этим угрозы экономической и информационной безопасности необходимо классифицировать с тем, чтобы наиболее полно и адекватно проводить указанную идентификацию: *по* источнику угрозы, *по* природе возникновения, *по* вероятности реализации, *по* отношению к виду человеческой деятельности, *по* объекту посягательства, *по* последствиям, *по* возможностям прогнозирования.

Угрозы можно классифицировать *по* нескольким критериям:

* по важнейшим составляющим информационной безопасности (доступность, целостность, конфиденциальность), против которых направлены угрозы в первую очередь;
* по компонентам информационных систем и технологий (данные, программно-аппаратные комплексы, сети, поддерживающая инфраструктура), на которые угрозы непосредственно нацелены;
* по способу осуществления (случайные или преднамеренные действия, события техногенного или природного масштаба);
* по локализации источника угроз (вне или внутри информационной технологии или системы).

Одна из возможных моделей классификации угроз представлена на [рис. 2.1](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27498?page=1#image.2.1) [Вихорев, С., Кобцев Р., 2002].



**Рис. 2.1.**Модель возможных угроз системе информационной безопасности и основные классы методов защиты

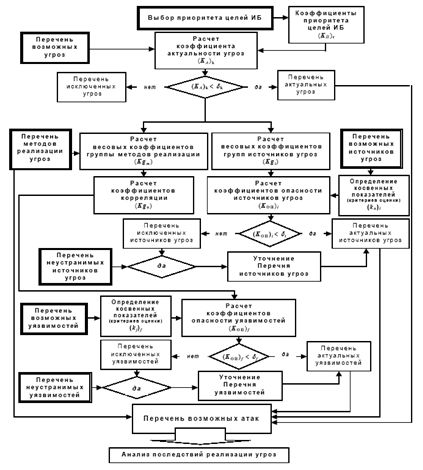
В ходе анализа необходимо убедиться, что большинство возможных источников угроз и уязвимости идентифицированы и сопоставлены друг с другом, а всем идентифицированным источникам угроз и уязвимостям сопоставлены методы их нейтрализации и устранения.

Указанная классификация может служить основой для выработки методики оценки актуальности той или иной угрозы, и при обнаружении наиболее актуальных угроз могут приниматься меры *по* выбору методов и средств для их предотвращения или нейтрализации.

При выявлении актуальных угроз экспертно-аналитическим методом определяются объекты защиты, подверженные воздействию той или иной угрозы, характерные источники этих угроз и уязвимости, способствующие реализации угроз.

На основании анализа составляется *матрица* взаимосвязи источников угроз и уязвимостей, из которой определяются возможные последствия реализации угроз (атаки) и вычисляется коэффициент значимости (степени опасности) этих атак как *произведение* коэффициентов опасности соответствующих угроз и источников угроз, определенных ранее.

Один из возможных алгоритмов проведения такого анализа, который легко формализуется и алгоритмизируется, показан на [рис. 2.2](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27498?page=1#image.2.2).



**Рис. 2.2.**Алгоритм проведения анализа и оценки угроз

Благодаря такому подходу возможно:

* установить приоритеты целей безопасности для субъекта отношений;
* определить перечень актуальных источников угроз;
* определить перечень актуальных уязвимостей;
* оценить взаимосвязь уязвимостей, источников угроз, возможности их осуществления;
* определить перечень возможных атак на объект;
* разработать сценарии возможных атак;
* описать возможные последствия реализации угроз;
* разработать комплекс защитных мер и систему управления экономической и информационной безопасностью предприятия.

Выше было отмечено, что самыми частыми и самыми опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих *информационные системы*. Иногда такие ошибки и являются собственно угрозами (неправильно введенные данные или ошибка в программе, вызвавшая крах системы), иногда они создают уязвимые места, которыми могут воспользоваться злоумышленники (таковы обычно ошибки администрирования). *По* некоторым данным, до 65% потерь возникают из-за непреднамеренных ошибок, совершенных *по* неосторожности, халатности или несоответствующей подготовки персонала.

Обычно пользователи могут быть источниками следующих угроз:

* намеренная (встраивание логической бомбы, которая со временем разрушит программное ядро или приложения) или непреднамеренная потеря или искажение данных и информации, "взлом" системы администрирования, кража данных и паролей, передача их посторонним лицам и т.д.;
* нежелание пользователя работать с информационной системой (чаще всего проявляется при необходимости осваивать новые возможности или при расхождении между запросами пользователей и фактическими возможностями и техническими характеристиками) и намеренный вывод из строя её программно-аппаратных устройств;
* невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т. п.).

Очевидно, что эффективный способ борьбы с непреднамеренными ошибками — максимальная *автоматизация* и стандартизация, информационных процессов, использование устройств "защита от дурака" (Fool *Proof* *Device*), регламентация и строгий *контроль* действий пользователей. Необходимо также следить за тем, чтобы при увольнении сотрудника его *права доступа* (логического и физического) к информационным ресурсам аннулировались.

Основными источниками внутренних системных отказов являются:

* невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т. п.);
* отступление (случайное или умышленное) от установленных правил эксплуатации;
* выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т. п.);
* ошибки конфигурирования системы;
* отказы программного и аппаратного обеспечения;
* разрушение данных;
* разрушение или повреждение аппаратуры.

*По* отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

* нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования;
* разрушение или повреждение помещений;
* невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т. п.).

Опасны, разумеется, *стихийные бедствия* (наводнения, землетрясения, ураганы) и события, являющиеся результатом техногенных катастроф (пожары, взрывы, обрушения зданий и т.д.). *По* статистике, на долю огня, воды и тому подобных "злоумышленников" (среди которых самый опасный — сбой электропитания) приходится 13-15% потерь, нанесенных производственным информационным системам и ресурсам.

Результаты проведения оценки и анализа могут быть использованы при выборе адекватных оптимальных методов парирования угроз, а также при аудите реального состояния информационной безопасности объекта.

Для создания оптимальной системы информационной безопасности предприятия необходимо грамотно оценить ситуацию, выявить возможные риски, разработать концепцию и политику безопасности, на основе которых строится модель системы и вырабатываются соответствующие *механизмы* реализации и функционирования.

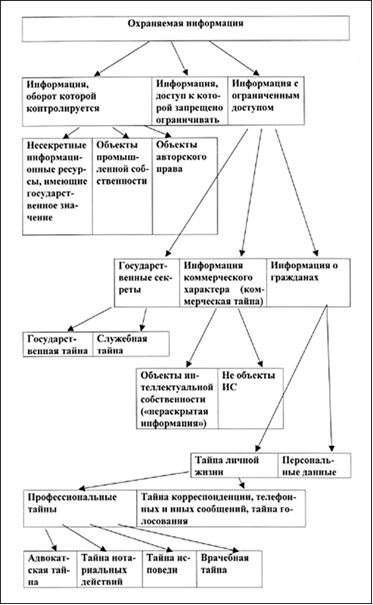
**Основные виды защищаемой информации**

Любое предприятие, получающее ресурсы, в том числе и информационные, перерабатывает их в продукты своей деятельности. При этом оно порождает специфическую внутреннюю среду, которая формируется совокупностью структурных подразделений, персоналом, техническими средствами и технологическими процессами, экономическими и социальными отношениями как внутри предприятия, так и во взаимодействии с внешней средой.

Совокупность внешней и внутренней информации, обслуживающие системы и технологии, ИТ-специалисты и персонал ИТ-подразделений составляют информационно-технологический *ресурс* (*Information* & *Technology* *Resource* — ITR) современного предприятия.

Внутри предприятия информационные потоки поступают в соответствующие модули корпоративной системы для структурирования, систематизации, обработки, анализа и практического использования. Большая часть этой информации является свободно используемой в процессе реализации деятельности государственного или коммерческого предприятия, однако в зависимости от особенностей внутренней деятельности и взаимодействия с внешним миром часть информации может быть "для служебного пользования", "строго конфиденциальной" или "секретной". Такая *информация* является, как правило, "закрытой" и требует соответствующих мер защиты ([рис. 2.3](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27498?page=2#image.2.3)).

Для коммерческих компаний используются достаточно простые категории и виды информации ([табл. 1](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27498?page=2#table.1) и [табл. 2](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27498?page=2#table.2)).



**Рис. 2.3.**Общая классификация охраняемой информации

Однако в любом случае статус определенного вида информации должен быть закреплен в соответствующем нормативном документе *по* безопасности и известен всем участникам управленческой, организационной и производственной деятельности.

Для обеспечения безопасности при работе с охраняемой информацией следует, во-первых, выстроить политику работы с конфиденциальной и служебной информацией, разработать и издать соответствующие политики, руководства и процедуры и, во-вторых, обеспечить необходимые программно-аппаратные ресурсы.

Первый шаг — это введение коммерческой тайны в соответствии с федеральным законом N 98-ФЗ "О коммерческой тайне" . Положение о коммерческой тайне разрабатывается департаментом (отделом) информационной безопасности предприятия и вводится приказом генерального директора.

Примерная процедура документирования состоит из разработки и использования следующих документов:

* положение о коммерческой тайне;
* приказ генерального директора о введении коммерческой тайны в компании;
* приказ генерального директора о назначении ответственных за соблюдение коммерческой тайны;
* перечень сведений, составляющих коммерческую тайну;
* учет носителей коммерческой тайны (журналы, грифы);
* приказ генерального директора об ответственности за разглашение или несанкционированную передачу коммерческой тайны.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Таблица 1. Категории деловой информации | | | | |
| **Раздел классификации** | | **Категория информации** | | |
| Общедоступная (Public) | | Открытая информация, при работе с которой нет никаких ограничений | | |
| Для служебного пользования (Restricted Access) | | Информация ограниченного доступа | | |
| Конфиденциальная (Confidential) | | Конфиденциальная информация, при работе с которой вводятся строгие ограничения в зависимости от уровней допуска пользователя | | |
| Персональная (Private) | | Персональная информация (зарплатная ведомость, адресные и паспортные данные сотрудников, медицинские карточки, ИНН, СПС и пр.) | | |
| Таблица 2. | | | | |
| **Вид информации** | **Содержание** | | **Расположение** | **Гриф** |
| Регистрационная, уставная, юридическая, нормативная | Регистрационные и уставные документы, нормативы | | Локально, базы данных системы поддержки деятельности руководителей и база юридической подсистемы | Для служебного пользования, конфиденциальная |
| Плановая, научно-исследовательская и общая производственная | Планы производства, описание технологий, внутренние разработки, стандарты, спецификации, интеллектуальная собственность | | Локально, производственные базы данных, файловые серверы | Для служебного пользования, конфиденциальная |
| Инфраструктурная | Карты и журналы ИТ-инфра-структуры, ИТ-системы, системы доступа | | Локально, файловый сервер | Для служебного пользования, конфиденциальная |
| Финансовые данные и управленческий учёт | Любая бухгалтерская информация, финансовые планы, отчеты, балансы, платежные документы | | Локально, база финансовой подсистемы либо другая среда работы финансового отдела | Для служебного пользования, конфиденциальная |
| Кадровая | Личные карточки персонала | | Локально, файловый сервер | Для служебного пользования, конфиденциальная |
| Текущая рабочая | Файлы и документы для внутреннего обмена данными | | Общедоступно, общий сервер | Общедоступная, для служебного пользования |
| Внутрикорпоративная | Приказы, распоряжения, расписания, отчеты собраний проектных групп, документы системы качества (планы, результаты проверок, корректирующие мероприятия) | | Общедоступно, общий сервер | Общедоступная, для служебного пользования |
| Развлекательная | Фотографии, видеоролики, фильмы, аудиокниги | | Общедоступно, общий либо выделенный сервер | Общедоступная |

В продолжение, необходимо создать набор политик *по* реализации внутренней информационной безопасности:

* политика информационной безопасности;
* политика предоставления прав доступа к внутренним и удаленным ресурсам;
* политика использования Internet/Intranet;
* политика использования электронной почты;
* порядок инвентаризации информационных ресурсов;
* соглашение о неразглашении данных и информации, составляющих коммерческую тайну и имеющих грифы "конфиденциально" и "для служебного пользования".

Программно-аппаратные средства для работы с охраняемой информацией либо встраиваются в соответствующие модули корпоративной информационной системы (КИС), либо используются локально в системах, оговоренных в политике ИБ. Средства противодействия угрозам ИБ и утечкам данных и информации являются, *по* сути, программно-аппаратным "слоем" между существующей ИТ-инфраструктурой предприятия и корпоративными приложениями, где обрабатываются конфиденциальные данные и с которыми работают сотрудники.

Защитный комплекс состоит не только из технических устройств и *ПО*, но и из совокупности организационных мер *по* реализации политики внутренней безопасности — целостное решение связывает воедино инфраструктуру, информацию и персонал.

В таком комплексе сочетаются все важные свойства, характерные для больших вычислительных и сетевых структур:

* многопоточность (по нескольким процессам на одном процессоре, по нескольким процессорам на одном сервере, распределение сложных задач обеспечения контроля и безопасности по разным серверам, использование вычислительных кластеров);
* физическое разделение on-line и off-line функций;
* повсеместная кластеризация и масштабирование, возможность выстраивать распределенные защитные схемы, располагая мониторинг в филиалах, а единое хранилище в главном офисе;
* возможность мониторинга всех каналов с помощью одной базы контентной фильтрации и единого журнала учёта доступа пользователей.

Такие целостные программные продукты осуществляют *контроль* и *управление рисками* внутренней безопасности и минимизируют утечки конфиденциальной информации, за счет соответствующих технологических составляющих, глубоко интегрированных в информационную структуру предприятия. К ним относятся программно-аппаратные устройства, осуществляющие:

* отслеживание перемещения конфиденциальной информации по информационной системе (Data-in-Shell);
* управление контролем утечки данных через сетевой трафик по протоколам TCP/IP, SMTP, HTTP(s), IM (ICQ, AOL, MSN), FTP, SQL, собственных протоколов посредством контентной фильтрации на уровне:
  + шлюза, через которые идет трафик из внутренней сети во внешнюю сеть (Data-in-Motion);
  + сервера, обрабатывающего определенный тип трафика (Data-at-Rest);
  + рабочей станции (Data-in-Use);
  + внутренних каналов почты Microsoft Exchange, Lotus Notes и др.
* управление контролем утечки охраняемой информации с рабочих станций, периферийных и мобильных устройств посредством контроля действий авторизованных пользователей с конфиденциальными данными: с файлами, внешними устройствами, сетью (локальной, беспроводной), буфером обмена, приложениями, устройств печати (локальные, сетевые);
* установление проактивной защиты и персональных сетевых экранов;
* теневое копирование информационных объектов в единую базу контентной фильтрации для всех каналов по единым правилам для всех каналов.

Грамотно организовать защиту охраняемых данных и информации непросто и недёшево. Для этого нужно произвести классификацию данных, тщательную инвентаризацию информационных ресурсов, выбрать адекватное программно-аппаратное решение, разработать и внедрить совокупность регламентирующих документы внутренней безопасности. Главную роль в этой непростой работе *по* минимизации рисков утечки данных играют компетентность и воля высшего руководства предприятия, актуальные политики и эффективные *программные средства*, а также *режим коммерческой тайны* при работе с охраняемой информацией.