Парадигма информационной безопасности

- ***Парадигма*** (от греческого пример, образец)
- 1)строго научная теория, воплощенная в системе понятий, выражающих существенные черты действительности;
- 2) исходная, концептуальная схема, модель постановки проблем и их решения, методов исследования, господствующих в течение определенного исторического периода в научном сообществе.

- Парадигма безопасности опирается на следующие *базовые* понятия: «актив», «собственник», «злоумышленник», «угроза», «уязвимость», «риск», «политика безопасности», «управление безопасностью», «мониторинг».

группы мер защиты

- правовые, устанавливающие юридические нормы владения, управления и ответственности при обладании активами;
- организационно-административные, регламентирующие и определяющие порядок работ по обеспечению безопасности всех субъектов;
- программные, реализующие в программной среде политику безопасности путем выполнения специальных настроек на оборудовании;
- •технические, реализующие политику безопасности техническими средствами.

постулаты парадигмы безопасности

- 1. В основе парадигмы безопасности лежит противоборство собственника и злоумышленника за контроль над активами. В случае если злоумышленник устанавливает контроль над активами, собственнику неминуемо наносится ущерб. Например, в банке, активы которого формируются за счет привлечения средств клиентов, ущерб наносится клиентам.

- 2. Главный источник угроз — собственный персонал (в технических терминах — авторизованный, то есть официально допущенный к активу; в нашем случае это пользователи, допущенные к работе с информацией и с информационными системами). Внешний злоумышленник (субъект несанкционированного доступа), вероятнее всего, имеет сообщника внутри организации.

- 3. Собственник никогда не знает наверняка о готовящемся нападении. Момент нападения для него всегда оказывается неожиданным.

- 4. Злоумышленник изучает объект нападения как теоретически (никак себя не обнаруживая), так и практически (путем исследования объекта и его системы безопасности). Таким образом, он находит точки уязвимости в системе защиты и с учетом этих знаний отрабатывает наиболее эффективный алгоритм атаки. Чем сложнее объект нападения, тем тщательнее он должен быть изучен и тем больше следов своей активности оставит злоумышленник.
- Авторизованный пользователь маскирует активность под служебную деятельность, а субъект НСД просто оставляет следы своей деятельности.

- 5. Поэтому собственник должен постоянно стремиться к выявлению следов такой активности.

- 6. Атаки злоумышленника, как правило, носят характер локальный и конкретный по месту, цели и времени. Также, как правило, локальны и конкретны угрозы природного характера, хотя по своей разрушительной силе они часто бывают исключительно сильны. Однако именно локальность катастроф такого типа дает возможность обеспечить высокую катастрофо устойчивость системы в целом, создавая и размещая резервные центры обработки данных (центры резервного копирования информации) на достаточном удалении друг от друга.

- 7. Однако сложно и исключительно ресурсоемко (следовательно, затратно и малоэффективно) искать следы активности потенциального субъекта угроз везде и по факту корректировать работу собственной системы защиты. Поэтому главный инструмент собственника — прогноз, основанный на опыте. Лучше всего, когда используется собственный опыт. Прогноз осуществляется путем составления модели угроз и модели субъекта угроз. В данном контексте специально использовано понятие «субъект угроз» вместо понятия «злоумышленник» потому что понятие «субъект угроз» включает в себя все возможные источники угроз, начиная от злонамеренной деятельности и заканчивая неграмотной эксплуатацией техники кондиционирования машинных залов. Чем точнее сделан прогноз, тем ниже риски нарушения безопасности при минимальных материальных и ресурсных затратах.

- 8. Следует отдавать себе отчет, что ни один риск в принципе нельзя уменьшить до нуля. Всегда будет оставаться некий остаточный риск. Задача минимизации рисков заключается в правильном определении уровня остаточного риска и его учете в практической деятельности. Однако часто бывает так, что остаточный риск вдруг резко увеличивается до неприемлемого уровня и может нанести вполне реальный ущерб. Так происходит, например, когда появляется новый компьютерный вирус, незнакомый средствам антивирусной защиты.

- 9. Наиболее правильный и эффективный способ минимизировать риски безопасности — на основе правильно сделанного прогноза разработать политику безопасности, отвечающую интересам собственника, и в соответствии с ней построить систему безопасности. Такая система безопасности способна выдержать практически все известные атаки, актуальные для актива, который защищает собственник.

- 10. Однако далеко не каждый собственник располагает необходимым потенциалом и достаточным опытом для подготовки грамотного прогноза. Поэтому прогноз может составляться на корпоративной основе, централизованно, с учетом опыта ведущих специалистов по обеспечению безопасности, например, в банковской сфере, а также с учетом международного опыта. Также на корпоративной основе, централизованно могут разрабатываться и основные требования по безопасности, определяющие общий для всех субъектов банковской деятельности необходимый и достаточный уровень безопасности.

- 11. Политика безопасности должна разрабатываться конкретно для каждого собственника, с учетом его особенностей, масштаба организации, **степени зрелости процессов управления** безопасностью и информационными ресурсами.

- 12. Соблюдение мер безопасности в значительной степени является элементом корпоративной и личной этики, поэтому на общий уровень безопасности организации оказывает большое влияние личное «зрелое» отношение сотрудника к своим собственным обязанностям и к бизнесу организации, а также взаимоотношения сотрудников внутри коллектива и между коллективом и собственником. Всем этим необходимо управлять и проводить ясную кадровую политику.

- 13. Меры по реализации выбранной политики безопасности должны финансироваться в достаточном объеме.
- 14. Собственник может убедиться в том, что средства расходуются правильно, проведя аудит расходования средств.

- 15. Технические меры защиты в силу ряда причин имеют некоторую тенденцию к ослаблению, в результате чего общий уровень безопасности организации может со временем незаметно для ее руководителей существенно снизиться. Это неминуемо ведет к росту рисков безопасности, что допустить нельзя. Следовательно, необходимо проводить постоянный мониторинг системы безопасности и своевременно принимать меры по поддержанию эффективности системы на требуемом уровне (управлению рисками).

- 16. Мониторинг должен быть эффективным (то есть максимально ресурсоемким и информативным), а также адекватным объекту защиты.
- 17. Таким образом, стратегия обеспечения безопасности заключается в превентивном создании системы безопасности, построенной в соответствии с выбранной политикой безопасности и противостоящей любым угрозам, учтенным в политике безопасности.