Муниципальное общеобразовательное учреждение
средняя общеобразовательная школа № 12
городского округа Самара

ДОКЛАД

для выступления на педагогическом совете
на тему:
«Организация открытого
безопасного информационного
пространства»

Подготовил:
Гальчинский В.А.

САМАРА
3 ноября 2009

ОГЛАВЛЕНИЕ

1. Введение

Для более точного понимания данной проблемы дадим несколько ключевых определений.

ОТКРЫТЫЙ - свободный для доступа (Толковый словарь русского языка Ушакова).

БЕЗОПАСНЫЙ - надежно защищенный, защищающий от опасностей (там же).

ИНФОРМАЦИЯ - сообщение, осведомляющее о положении дел или о чьей-нибудь деятельности, сведения о чем-нибудь (там же).

ИНФОРМАЦИОННОЕ ПРОСТРАНСТВО - совокупность данных, технологий их сопровождения и использования, информационных телекоммуникационных систем, функционирующих на основе общих принципов и обеспечивающих: информационное взаимодействие организаций и граждан и удовлетворение их информационных потребностей.

Основными компонентами информационного пространства являются: информационные ресурсы, средства информационного взаимодействия и информационная инфраструктура (Словарь по экономике и финансам – Глоссарий.Ру)

Итак, что же такое открытое безопасное информационное пространство?

Исходя из выше приведённых определений, это свободное для доступа, надёжно защищённое пространство, представляющее собой совокупность данных, технологий их сопровождения и использования, информационных телекоммуникационных систем.

Так насколько же открытым может быть информационное пространство, чтобы одновременно оставаться БЕЗОПАСНЫМ?

Для того, чтобы ответить на этот ключевой вопрос, рассмотрим понятие ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ более подробно.

Под информационной безопасностью мы будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

2. Основные составляющие информационной безопасности

Информационная безопасность – многогранная, можно даже сказать, многомерная область деятельности, в которой успех может принести только системный, комплексный подход.

Спектр интересов субъектов, связанных с использованием информационных систем, можно разделить на следующие категории: обеспечение **доступности**, **целостности** и **конфиденциальности** информационных ресурсов и поддерживающей инфраструктуры.

Доступность (далее ОТКРЫТОСТЬ) – это возможность за приемлемое время получить требуемую информацию. Под **целостностью** подразумевается актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения. Наконец, **конфиденциальность** – это защита от несанкционированного доступа к информации.

3. Важность и сложность проблемы информационной безопасности

Информационная безопасность является одним из важнейших аспектов интегральной безопасности, на каком бы уровне мы ни рассматривали последнюю – национальном, отраслевом, корпоративном или персональном.

Для иллюстрации этого положения ограничимся несколькими примерами.

- В **Доктрине информационной безопасности Российской Федерации** защита от несанкционированного доступа к информационным ресурсам, обеспечение безопасности информационных и телекоммуникационных систем выделены в качестве важных составляющих национальных интересов РФ в информационной сфере.
- Заместитель начальника управления по экономическим преступлениям Министерства внутренних дел России сообщил, что российские хакеры с 1994 по 1996 год предприняли почти 500 попыток проникновения в компьютерную сеть Центрального банка России. В 1995 году ими было похищено 250 миллиардов рублей (ИТАР-ТАСС, АР, 17 сентября 1996 года).
- В середине июля 1996 года корпорация General Motors отозвала 292860 автомобилей марки Pontiac, Oldsmobile и Buick моделей 1996 и 1997 годов, поскольку ошибка в программном обеспечении двигателя могла привести к пожару.
- В феврале 2001 года двое бывших сотрудников компании Commerce One, воспользовавшись паролем администратора, удалили с сервера файлы, составлявшие крупный (на несколько миллионов долларов) проект для иностранного заказчика. К счастью, имелась резервная копия проекта, так что реальные потери ограничились расходами на следствие и средства защиты от подобных инцидентов в будущем. В августе 2002 года преступники предстали перед судом.

Понятно, что подобных примеров множество, можно вспомнить и другие случаи – недостатка в нарушениях ИБ нет и не предвидится.

Приведем еще несколько цифр. В марте 1999 года был опубликован очередной, четвертый по счету, годовой отчет "Компьютерная преступность и безопасность-1999: проблемы и тенденции" (Issues and Trends: 1999 CSI/FBI Computer Crime and Security Survey). В отчете отмечается резкий рост числа обращений в правоохранительные органы по поводу компьютерных преступлений (32% из числа опрошенных); 30% респондентов сообщили о том, что их информационные системы были взломаны внешними злоумышленниками; атакам через Internet подвергались 57% опрошенных; в 55% случаях отмечались нарушения со стороны собственных сотрудников. **Примечательно, что 33% респондентов на вопрос "были ли взломаны ваши Web-серверы и системы электронной коммерции за последние 12 месяцев?" ответили "не знаю".**

Столь же тревожные результаты содержатся в обзоре InformationWeek, опубликованном 12 июля 1999 года. Лишь 22% респондентов заявили об отсутствии нарушений информационной безопасности. Наряду с распространением вирусов отмечается резкий рост числа внешних атак.

Увеличение числа атак – еще не самая большая неприятность. Хуже то, что постоянно обнаруживаются новые уязвимые места в программном обеспечении (выше мы указывали на ограниченность современной технологии программирования) и, как следствие, появляются новые виды атак.

Так, в информационном письме Национального центра защиты инфраструктуры США (National Infrastructure Protection Center, NIPC) от 21 июля 1999 года сообщается, что за период с 3 по 16 июля 1999 года выявлено девять проблем с ПО, риск использования которых оценивается как средний или высокий (общее число обнаруженных уязвимых мест равно 17). Среди "пострадавших" операционных платформ – почти все разновидности ОС Unix, Windows, MacOS, так что никто не может чувствовать себя спокойно, поскольку новые ошибки тут же начинают активно использоваться злоумышленниками.

В таких условиях системы информационной безопасности должны уметь противостоять разнообразным атакам, как внешним, так и внутренним, атакам автоматизированным и скоординированным. Иногда нападение длится доли секунды; порой прощупывание уязвимых мест ведется медленно и растягивается на часы, так что подозрительная активность практически незаметна. Целью злоумышленников может быть нарушение всех составляющих ИБ – доступности, целостности или конфиденциальности.

4. Основные определения и критерии классификации угроз

Угроза - это потенциальная возможность определенным образом нарушить информационную безопасность.

Попытка реализации угрозы называется **атакой**, а тот, кто предпринимает такую попытку, - **злоумышленником**. Потенциальные злоумышленники называются **источниками угрозы.**

Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем (таких, например, как возможность доступа посторонних лиц к критически важному оборудованию или ошибки в программном обеспечении).

Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется **окном опасности**, ассоциированным с данным уязвимым местом. Пока существует окно опасности, возможны успешные атаки на ИС.

Если речь идет об ошибках в ПО, то окно опасности "открывается" с появлением средств использования ошибки и ликвидируется при наложении заплат, ее исправляющих.

Угрозы можно классифицировать по нескольким критериям:

- по аспекту информационной безопасности (доступность, целостность, конфиденциальность), против которого угрозы направлены в первую очередь;
- по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);
- по способу осуществления (случайные/преднамеренные, действия природного/техногенного характера);
- по расположению источника угроз (внутри/вне рассматриваемой ИС).

В качестве основного критерия мы будем использовать первый (по аспекту ИБ), привлекая при необходимости остальные.

4.1. Наиболее распространенные угрозы доступности

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 - следствие непреднамеренных ошибок.

Пожары и наводнения не приносят столько бед, сколько безграмотность и небрежность в работе.

Очевидно, самый радикальный способ борьбы с непреднамеренными ошибками - максимальная автоматизация и строгий контроль.

Другие угрозы доступности классифицируем по компонентам ИС, на которые нацелены угрозы:

- отказ пользователей;
- внутренний отказ информационной системы;
- отказ поддерживающей инфраструктуры.

Обычно применительно к пользователям рассматриваются следующие угрозы:

- нежелание работать с информационной системой (чаще всего проявляется при необходимости осваивать новые возможности и при расхождении между запросами пользователей и фактическими возможностями и техническими характеристиками);
- невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т.п.);
- невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т.п.).

Основными источниками внутренних отказов являются:

- 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 при (пере)конфигурировании 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.)

4.2. Вредоносное программное обеспечение

Одним из опаснейших способов проведения атак является внедрение в атакуемые системы вредоносного программного обеспечения.

Мы выделим следующие грани вредоносного ПО:

- вредоносная функция;
- способ распространения;
- внешнее представление.

Часть, осуществляющую разрушительную функцию, будем называть "бомбой" (хотя, возможно, более удачными терминами были бы "заряд" или "боеголовка"). Вообще говоря, спектр вредоносных функций неограничен, поскольку "бомба", как и любая другая программа, может обладать сколь угодно сложной логикой, но обычно "бомбы" предназначаются для:

- внедрения другого вредоносного ПО;
- получения контроля над атакуемой системой;
- агрессивного потребления ресурсов;
- изменения или разрушения программ и/или данных.

По механизму распространения различают:

- вирусы - код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы;
- "черви" - код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение (для активизации вируса требуется запуск зараженной программы).

Вирусы обычно распространяются локально, в пределах узла сети; для передачи по сети им требуется внешняя помощь, такая как пересылка зараженного файла. "Черви", напротив, ориентированы в первую очередь на путешествия по сети.

Иногда само распространение вредоносного ПО вызывает агрессивное потребление ресурсов и, следовательно, является вредоносной функцией. Например, "черви" "съедают" полосу пропускания сети и ресурсы почтовых систем. По этой причине для атак на доступность они не нуждаются во встраивании специальных "бомб".

Вредоносный код, который выглядит как функционально полезная программа, называется троянским. Например, обычная программа, будучи пораженной вирусом, становится троянской; порой троянские программы изготавливают вручную и подсовывают доверчивым пользователям в какой-либо привлекательной упаковке.

Окно опасности для вредоносного ПО появляется с выпуском новой разновидности "бомб", вирусов и/или "червей" и перестает существовать с обновлением базы данных антивирусных программ и наложением других необходимых заплат.

По традиции из всего вредоносного ПО наибольшее внимание общественности приходится на долю вирусов. Однако до марта 1999 года с полным правом можно было утверждать, что "несмотря на экспоненциальный рост числа известных вирусов, аналогичного роста количества инцидентов, вызванных ими, не зарегистрировано. Соблюдение несложных правил "компьютерной гигиены" практически сводит риск заражения к нулю. Там, где работают, а не играют, число зараженных компьютеров составляет лишь доли процента".

Таким образом, действие вредоносного ПО может быть направлено не только против доступности, но и против других основных аспектов информационной безопасности.

4.3. Основные угрозы целостности

На втором месте по размерам ущерба (после непреднамеренных ошибок и упущений) стоят кражи и подлоги. По данным газеты USA Today, еще в 1992 году в результате подобных противоправных действий с использованием персональных компьютеров американским организациям был нанесен общий ущерб в размере 882 миллионов долларов. Можно предположить, что реальный ущерб был намного больше, поскольку многие организации по понятным причинам скрывают такие инциденты; не вызывает сомнений, что в наши дни ущерб от такого рода действий вырос многократно.

В большинстве случаев виновниками оказывались штатные сотрудники организаций, отлично знакомые с режимом работы и мерами защиты. Это еще раз подтверждает опасность внутренних угроз, хотя говорят и пишут о них значительно меньше, чем о внешних.

Ранее мы проводили различие между статической и динамической целостностью. С целью нарушения статической целостности злоумышленник (как правило, штатный сотрудник) может:

- ввести неверные данные;
- изменить данные.

Потенциально уязвимы с точки зрения нарушения **целостности** не только **данные**, но и **программы**. Внедрение рассмотренного выше вредоносного ПО - пример подобного нарушения.

Угрозами динамической целостности являются нарушение атомарности транзакций, переупорядочение, кража, дублирование данных или внесение дополнительных сообщений (сетевых пакетов и т.п.). Соответствующие действия в сетевой среде называются активным прослушиванием.

4.4. Основные угрозы конфиденциальности

Конфиденциальную информацию можно разделить на предметную и служебную. Служебная информация (например, пароли пользователей) не относится к определенной предметной области, в информационной системе она играет техническую роль, но ее раскрытие особенно опасно, поскольку оно чревато получением несанкционированного доступа ко всей информации, в том числе предметной.

Даже если информация хранится в компьютере или предназначена для компьютерного использования, угрозы ее конфиденциальности могут носить некомпьютерный и вообще нетехнический характер.

Многим людям приходится выступать в качестве пользователей не одной, а целого ряда систем (информационных сервисов). Если для доступа к таким системам используются многоразовые пароли или иная конфиденциальная информация, то наверняка эти данные будут храниться не только в голове, но и в записной книжке или на листках бумаги, которые пользователь часто оставляет на рабочем столе, а то и попросту теряет. И дело здесь не в неорганизованности людей, а в изначальной непригодности парольной схемы. Невозможно помнить много разных паролей; рекомендации по их регулярной (по возможности - частой) смене только усугубляют положение, заставляя применять несложные схемы чередования или вообще стараться свести дело к двум-трем легко запоминаемым (и столь же легко угадываемым) паролям.

Еще один пример изменения, о котором часто забывают, - хранение данных на резервных носителях. Для защиты данных на основных носителях применяются развитые системы управления доступом; копии же нередко просто лежат в шкафах и получить доступ к ним могут многие.

Таковы основные угрозы, которые наносят наибольший ущерб субъектам информационных отношений.

5. Возможное решение проблемы

Успех в области информационной безопасности может принести только комплексный подход, сочетающий меры четырех **уровней**:

- **законодательного**;
- **административного**;
- **процедурного**;
- **программно-технического**.

5.1

Законодательный уровень является важнейшим для обеспечения информационной безопасности. Необходимо всячески подчеркивать важность проблемы ИБ; сконцентрировать ресурсы на важнейших направлениях исследований; скоординировать образовательную деятельность; создать и поддерживать негативное отношение к нарушителям ИБ - все это функции законодательного уровня.

На законодательном уровне особого внимания заслуживают **правовые акты** и **стандарты**.

Российские правовые акты в большинстве своем имеют ограничительную направленность. Сами по себе **лицензирование** и **сертификация** не обеспечивают безопасности. К тому же в законах не предусмотрена ответственность государственных органов за нарушения ИБ. Реальность такова, что в России в деле обеспечения ИБ на помощь государства рассчитывать не приходится.

На этом фоне поучительным является знакомство с законодательством США в области ИБ, которое гораздо обширнее и многограннее российского.

Среди стандартов выделяются **"Оранжевая книга"**, рекомендации **X.800** и "Критерии оценки безопасности информационных технологий".

"Оранжевая книга" заложила понятийный базис; в ней определяются важнейшие **сервисы безопасности** и предлагается метод **классификации** информационных систем по требованиям безопасности.

Рекомендации X.800 весьма глубоко трактуют вопросы защиты **сетевых конфигураций** и предлагают развитый набор сервисов и **механизмов безопасности**.

Международный стандарт ISO 15408, известный как **"Общие критерии"**, реализует более современный подход, в нем зафиксирован чрезвычайно широкий спектр сервисов безопасности (представленных как **функциональные требования**). Его принятие в качестве национального стандарта важно не только из абстрактных соображений интеграции в

мировое сообщество; оно, как можно надеяться, облегчит жизнь владельцам информационных систем, существенно расширив спектр доступных сертифицированных решений.

5.2

Главная задача мер административного уровня - сформировать программу работ в области информационной безопасности и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Основой программы является **политика безопасности**, отражающая подход организации к защите своих информационных активов.

Разработка политики и **программы безопасности** начинается с **анализа рисков**, первым этапом которого, в свою очередь, является ознакомление с наиболее распространенными **угрозами.**

Главные угрозы - внутренняя сложность ИС, непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы.

На втором месте по размеру ущерба стоят кражи и подлоги.

Реальную опасность представляют пожары и другие аварии поддерживающей инфраструктуры.

В общем числе нарушений растет доля внешних атак, но основной ущерб по-прежнему наносят "свои".

Для подавляющего большинства организаций достаточно общего знакомства с рисками; ориентация на типовые, апробированные решения позволит обеспечить **базовый уровень безопасности** при минимальных интеллектуальных и разумных материальных затратах.

5.3

Меры процедурного уровня ориентированы на людей (а не на технические средства) и подразделяются на следующие виды:

- управление персоналом;
- физическая защита;
- поддержание работоспособности;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

На этом уровне применимы важные принципы безопасности:

- непрерывность защиты в пространстве и времени;

- разделение обязанностей;
- минимизация привилегий.

На этапе инициации сотрудника должно быть разработано описание должности с требованиями к квалификации и выделяемыми компьютерными привилегиями; на этапе установки необходимо провести обучение, в том числе по вопросам безопасности.

5.4

Программно-технические меры, то есть меры, направленные на контроль компьютерных сущностей - оборудования, программ и данных, образуют последний и самый важный рубеж информационной безопасности.

На этом рубеже становятся очевидными не только позитивные, но и негативные последствия быстрого прогресса информационных технологий. Во-первых, дополнительные возможности появляются не только у специалистов по ИБ, но и у злоумышленников. Во-вторых, информационные системы все время модернизируются, перестраиваются, к ним добавляются недостаточно проверенные компоненты (в первую очередь программные), что затрудняет соблюдение режима безопасности.

Меры безопасности целесообразно разделить на следующие виды:

- **превентивные**, препятствующие нарушениям ИБ;
- меры **обнаружения** нарушений;
- **локализующие**, сужающие зону воздействия нарушений;
- меры **восстановления** режима безопасности.

С практической точки зрения важными также являются следующие принципы архитектурной безопасности:

- непрерывность защиты в пространстве и времени, невозможность миновать защитные средства;
- следование признанным стандартам, использование апробированных решений;
- иерархическая организация ИС;
- усиление «**слабого звена»;**
- невозможность перехода в **небезопасное состояние**;
- минимизация привилегий;
- разделение обязанностей;
- разнообразие защитных средств;
- **простота** и **управляемость** информационной системы.

6. Заключение

Открытое и безопасное информационное пространство может существовать только при чётком обеспечении информационной безопасности. В данном процессе активное участие должны принимать все участники информационного процесса.

7. Использованные источники

- http://slovari.yandex.ru/
- http://ru.wikipedia.org
- http://www.securelist.com/ru/
- http://www.intuit.ru/