створюється реальна можливість порушення цілісності цієї інформації або її витоку технічними каналами; друга – невиконання норм і вимог технічного захисту комп'ютерної інформації, в результаті чого створюються передумови для порушення цілісності цієї інформації або її витоку; третя – невиконання інших вимог технічного захисту інформації з обмеженим доступом [2].

Про поняття "викрадення" комп'ютерної інформації, "перекручення чи знищення" комп'ютерної інформації вже йшлося вище. Викрадення комп'ютерної інформації може бути вчинене шляхом несанкціонованого доступу до неї, приймання й аналізу побічних електромагнітних випромінювань і наводок, використання закладних пристроїв.

Засоби захисту комп'ютерної інформації – це технічні пристрої і (або) технологічні розробки, призначені для створення технологічної перешкоди несанкціонованого доступу до комп'ютерної інформації.

Копіювання комп'ютерної інформації – це її відтворення у електронному вигляді, перенесення на інший носій інформації з використанням програмних та (або) технічних засобів АЕОМ. Копіювання комп'ютерної інформації без використання програмно-технічних засобів АЕОМ, наприклад, шляхом сканування випромінювання монітора спеціальним технічним засобом, має розглядатись як її викрадення.

Визнання порушення роботи КС істотно залежить від тривалості переривання їх роботи, складності і тривалості їх ремонту тощо.

Із **суб'єктивної сторони** злочин, передбачений ч. 1 ст. 363 КК, характеризується непрямим умислом чи необережністю щодо наслідків у вигляді викрадення, перекручення чи знищення комп'ютерної інформації, засобів її захисту, незаконного копіювання комп'ютерної інформації чи істотного порушення роботи КС. Саме ж порушення правил експлуатації КС може бути як умисним, так і необережним.

Суб'єкт злочину спеціальний – особа, яка відповідає за експлуатацію КС. До таких осіб відносяться особи, які безпосередньо здійснюють експлуатацію КС, управління ними, а також особи, які забезпечують належну їх експлуатацію або здійснюють їх обслуговування і на яких покладена відповідальність за належну їх експлуатацію. Це може бути оператор АЕОМ, особа технічного персоналу, на яку покладені обов'язки з забезпечення безпечної експлуатації АЕОМ, їх ремонту, профілактичного обслуговування, охорони від несанкціонованого доступу до них, забезпечення технічного захисту комп'ютерної інформації, її приховування та ін.

Кваліфікованим видом злочину є порушення правил експлуатації КС, якщо воно заподіяло **істотну шкоду**. Шкода може бути як матеріальною, так і не матеріальною.

Порушення правил експлуатації КС особою, яка відповідає за їх експлуатацію, з метою незаконного копіювання комп'ютерної інформації, її привласнення чи заволодіння нею службовою особою шляхом зловживання своїм службовим становищем, за відсутності інших наслідків, передбачених ст. 363 КК, має кваліфікуватися лише за ст. 362 КК, оскільки таке порушення є способом вчинення злочину, передбаченого ст. 362, і додаткової кваліфікації за ст. 363 КК не потребує. Якщо ж внаслідок зазначеного порушення матиме місце витік, викрадення, перекручення чи знищення комп'ютерної інформації, або викрадення засобів її захисту іншими особами, або істотне порушення роботи КС, то дії особи мають кваліфікуватися за сукупністю злочинів за ст. 362 та ст. 363 КК.

Література: 1. Закон України "Про захист інформації в автоматизованих системах" від 05. 07. 1994 р. // ЗУ. Том 7. – К., 1997. – С. 296. 2. Положення про технічний захист інформації в Україні, затв. постановою КМ України від 09. 09. 1994 р. № 632 // ЗП України. – 1994. – № 12. – С. 302. 3. Закон України "Про авторське право і суміжні права" від 23. 12. 1993 р. в ред. 11. 07. 2001 р. // ГУ, 2001, 16. 08. 4. Закон України "Про інформацію" від 02. 10. 1992 р. ст. 38. \\ ВВРУ, 1992, № 48, С. 650.

УДК 638.235.231

АУДИТ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – ПРОБЛЕМЫ И РЕШЕНИЯ

Юрий Борсуковский
Фирма «Бартек»

Аннотация: **Рассмотрены вопросы аудита систем информационной безопасности.**
Summary: **The audit questions of information safety are considered in the given report.**
Ключевые слова: **Информация, информационная безопасность, тест, аудит, обследование.**

I Введение

Эффективная работа современной компании немыслима без применения современных информационных технологий. Внедрение автоматизированных информационных систем дает ряд очевидных преимуществ (повышение управляемости, увеличение рентабельности и др.), и в то же самое время приводит, как правило, к увеличению объема конфиденциальной информации, обрабатываемой в электронном виде. И если не предпринимаются специальные меры по защите информации, то это влечет за собой снижение общего уровня безопасности компании, утечку конфиденциальной информации и, как следствие, прямые и весьма ощутимые убытки. Кроме того, динамика принятия решений и современное состояние информатизации общества требует для решения многих оперативных, коммерческих и управленческих задач активного использования глобальной сети Internet.

Решение о начале использования сети Internet для решения корпоративных задач требует от компании перехода на новые платформы и технологии для обеспечения таких операций. Для эффективной организации систем обработки данных и управления, систем электронной коммерции и построения сетей Extranet большинству компаний требуется коренная перестройка вычислительной системы с целью приведения ее в соответствие с современными стандартами и технологиями межкорпоративного взаимодействия.

Для тех, кто отвечает за информационную безопасность, решение о подключении корпоративной сети компании к Internet или о межкорпоративной интеграции знаменует собой начало совершенно новой эры, так как с этого момента их функции и проблемы, связанные с защитой конфиденциальной информации при использовании компьютерных систем, резко увеличивают свою актуальность.

Проблема защиты конфиденциальной информации имеет две стороны. Одна сторона – это защита информации внутри корпоративной системы, другая – это защита информации от вторжения извне, то есть вторжение в информационные системы через электронные каналы связи и каналы Internet.

Internet растет с головокружительной скоростью, поэтому нет ничего удивительного в том, что регистрируется все больше попыток несанкционированного доступа к корпоративным ресурсам. Планы таких атак не являются тайной, так что зачастую их можно найти прямо в готовом для применения формате, а недавние эксцессы, носившие поистине глобальный характер, – явное свидетельство того, что в целом совершить компьютерное преступление сегодня намного проще, чем раньше. И если прежде основную угрозу представлял тщательно организованный промышленный шпионаж, то теперь ему на смену приходят «воришки со сценариями», «проказы» которых, возможно, обойдутся вашей компании в многие тысячи долларов из-за простоя в результате проведения несложной, стандартной скрытой атаки.

Конечно, это не то, на чем можно сделать фильм о Джеймсе Бонде, но результаты могут оказаться столь же драматичными. В ежегодном опросе по поводу компьютерных преступлений и проблем безопасности Института компьютерной защиты (Computer Security Institute, CSI) 186 тех респондентов, кто указал размер ущерба от компьютерных вторжений, в 2001 г. понесли убытки в сумме на 369 млн. долларов. Это составляет в среднем по 1 987 тыс. долларов на компанию.

Прошли те времена, когда простой брандмауэр, был достаточно надежным средством защиты, чтобы администраторы сетей могли спокойно спать по ночам. Современные корпорации предусматривают сложные стратегии защиты, реализация которых предполагает использование нескольких систем, как предупредительных, так и реактивных (часто они являются многоуровневыми и избыточными). В этом новом мире Internet выявление атак становится столь же распространенным, как шифрование и аутентификация, и широко применяется как крупными, так и небольшими компаниями.

Отметим, что проблема защиты от внутренних угроз, задача обеспечения надежности работы и вопрос контроля целостности ресурсов существуют независимо от внешних связей корпоративной сети. По данным совместного опроса, проведенного в 2000 году Институтом защиты информации и ФБР США, 71% респондентов указывают на то, что инициаторами несанкционированного доступа к ресурсам сети были собственные сотрудники, и только 25% подвергались атакам извне [1]. Причем для взлома сети изнутри не надо быть специалистом высокого уровня. Для этого достаточно иметь небольшой опыт и недостаточно четко организованную систему информационной безопасности компании.

С интеграцией автоматизированных систем компании в Internet или в другие сети общего пользования актуальность безопасности только возрастает. Служба информационной безопасности компании должна в обязательном порядке участвовать в работах по созданию корпоративной системы с начала ее проектирования и до момента ввода в эксплуатацию.

Кроме того, уже работающую систему необходимо периодически обследовать на предмет выявления новых слабостей и рисков. Пренебрежение безопасностью корпоративных систем и надежда «на авось» неминуемо приводят к крупным финансовым потерям от реализации внутренних или внешних угроз. По оценкам и данным опросов, проведенных SANS Institute, убыток только от одной атаки на корпоративную

систему для банковского и IT-секторов экономики США (где безопасности уделяется особое внимание) составляет в среднем около 500 тыс. долларов.

Таким образом, проблема защиты информации существует и с каждым днем актуальность этой проблемы растет.

С какой стороны и как подходить к решению этой проблемы? Ведь для организации защиты информации или проведения аудита существующей автоматизированной системы необходим штат высококвалифицированных специалистов в области информационной безопасности (не надо их путать с разработчиками программного обеспечения и администраторами сетей). А это может быть очень дорого и невыгодно для организаций, особенно небольших.

Что можно порекомендовать в наших конкретных условиях? Для проведения обследований и аудита целесообразно привлекать сторонние специализированные компании, так как они имеют большой опыт и штат профессионалов в области обеспечения и контроля состояния информационной безопасности. Кроме того, они обеспечивают установку оборудования и специализированного программного обеспечения на условиях лизинга, а также выполняют работы по его постоянному обновлению и отслеживанию общего уровня системы информационной безопасности.

Такой подход позволяет решить массу проблем, как с финансовой точки зрения, так и организационной. Не надо забывать, что стоимость оборудования и стоимость специалистов по информационной безопасности исчисляется достаточно серьезными цифрами.

Кроме того, работа с такими компаниями позволят автоматически получать прецеденты и вести постоянное усовершенствование собственной системы безопасности на основании информации о проблемах, которые возникали с другими фирмами.

Рассмотрим, какие виды услуг предлагают такие компании в Украине, и оценим их с точки зрения полезности для достижения заданного уровня информационной безопасности.

II Виды услуг на информационном рынке Украины

Тест на преодоление защиты. Задача заключается в попытке обойти принятую в корпоративной сети систему безопасности. При этом фирма-консультант выступает в роли злоумышленника (внутреннего или внешнего), задача которого – условно скомпрометировать корпоративную систему, получить “конфиденциальные” данные или условно нарушить функционирование системы. Основными целями предпринимаемой попытки преодоления защиты являются констатация и доказательство возможности взлома системы, а также выявление реакции на атаку персонала (как администраторов, так и рядовых пользователей).

Успешная реализация атаки – действенное средство доказать руководству компании необходимость увеличения затрат на обеспечение информационной безопасности, особенно если в результате успешного взлома фирме-эксперту удалось незаконно получить какую-либо конфиденциальную информацию руководства. Кроме того, тест на преодоление защиты является хорошим способом проверить соблюдение персоналом принятой политики безопасности, например, правил хранения и смены пароля.

Недостатком данного метода является отсутствие в результате целостной картины состояния информационной безопасности. Заказчик лишь получает информацию о том, что исследуемая система уязвима. Проведение определенной атаки не позволяет выявить весь набор уязвимых и слабых мест системы и тем более не дает никаких рекомендаций по повышению уровня защищенности автоматизированной системы.

Аудит. Под аудитом подразумевается оценка текущего состояния компьютерной системы на соответствие некоему стандарту или предъявляемым требованиям. Стандарты могут быть внутрикорпоративными или общими (как государственными, так и коммерческими).

В большинстве случаев аудит требуется, когда автоматизированная система предназначена для обработки конфиденциальной или секретной информации. Для каждой категории информации стандартами определяется нижняя граница уровня безопасности автоматизированной системы.

Проведение аудита полезно также после построения автоматизированной системы и ее подсистем безопасности на этапе приемки в эксплуатацию – для оценки степени соблюдения предъявляемых к ней требований. Следует отметить, что аудит автоматизированной системы рекомендуется проводить периодически (например, раз в год), так как состояние любой системы изменяется с течением времени, и к моменту очередного аудита оно может не иметь ничего общего с тем, что было зафиксировано при предыдущем аудите.

Отчет об аудите содержит оценку соответствия системы данному стандарту, но не содержит рекомендаций и предложений по устранению выявленных уязвимых мест и повышению уровня защищенности.

Обследование. Оценка автоматизированной системы – наиболее сложный и полезный вид работ по обеспечению информационной безопасности. В рамках этой работы фирма-эксперт проводит комплексную оценку автоматизированной системы с учетом ее особенностей.

Такая оценка включает анализ информационных потоков аппаратного и программного обеспечения, сетевой инфраструктуры, методов управления и администрирования компонентов.

После сбора и упорядочивания информации специалисты фирмы-эксперта проводят анализ состояния информационной безопасности, состоящий из нескольких этапов:

- анализ существующей организационной структуры обеспечения информационной безопасности, в том числе анализ функций службы информационной безопасности;
- анализ взаимоотношений подразделений по вопросам обеспечения защиты информации, вопросов подчиненности и структуры службы информационной безопасности;
- анализ существующей нормативно-правовой базы информационной безопасности автоматизированной системы, в том числе оценка принятой политики безопасности, организационно-распорядительных документов, положений и инструкций по обеспечению защиты информации, а также анализ их соответствия существующим законодательным и нормативным актам;
- анализ мер технической защиты информации, в том числе анализ существующих мер и средств технической защиты информации, а также порядка их применения;
- рассмотрение и анализ используемых заказчиком средств разграничения доступа и защиты от несанкционированного доступа (в частности, при работе с Internet), антивирусных средств, межсетевых экранов, защиты с помощью паролей, системы обнаружения вторжений, криптографических средств защиты информации, методов контроля целостности и т. д.;
- анализируют порядок использования встроенных механизмов защиты компонентов в автоматизированной системе;
- оценивают достаточность мер и правильность использования средств технической защиты информации;
- производят выявление угроз безопасности (как внутренних, так и внешних) и определяют существующие уязвимые места в компонентах автоматизированной системы;
- производят оценку рисков для автоматизированной системы;
- ранжируют угрозы по вероятности их возникновения в данной автоматизированной системе и мере возможного ущерба от реализации угроз.

В результате фирма-эксперт предоставляет:

- список наиболее опасных угроз безопасности;
- перечень и описание уязвимых мест компонентов, включая описание их источников (модель нарушителя) и механизмов их реализации;
- рекомендации по доработке существующей системы защиты информации компании.

Рекомендации могут касаться совершенствования организационно-штатной структуры, доработки и создания нормативных документов, положений и инструкций по обеспечению информационной безопасности.

Кроме того, эксперты могут дать рекомендации по применению штатных средств защиты компонентов, а также по использованию дополнительных систем защиты информации и методов контроля и аудита состояния информационной безопасности.

Таким образом, обследование автоматизированных систем позволяет не только оценить степень уязвимости, но и укрепить подсистему информационной безопасности для защиты от угроз, исходящих как извне, так и изнутри, а также управлять рисками и минимизировать возможные потери.

III Выводы

Что происходит сегодня в области внедрения систем защиты информации в Украине? Можно выделить несколько ключевых факторов, на которые следует обратить внимание специалистов по информационной безопасности и руководства компаний.

Во-первых, покупается не то, что требуется, а на что хватает денег. Почему это происходит? Ответ достаточно очевиден. При внедрении систем информационной защиты забывают о том, что предварительно требуется разработать политику безопасности, определить факторы риска и только после этого начинать тратить деньги на приобретение программных и технических средств защиты информации. Кроме того, при разработке политики безопасности можно рассчитать потребный бюджет, осуществить его планирование и в соответствии с разработанной политикой безопасности эффективно расходовать выделяемые финансовые ресурсы на решение поставленных задач. Этого нет и, как следствие, получаем громадные затраты с очень низкой эффективностью.

Во-вторых. При принятии решений не учитывается, что внедрение системы защиты – это весьма длительный и кропотливый процесс. Бытует мнение, что после выделения финансовых средств на следующий день появится система безопасности. К сожалению, это не так. И чем раньше придет понимание этого, тем раньше прекратится неэффективная трата финансовых средств.

В-третьих. Разработка и внедрение полноценной системы защиты требует наличия квалифицированных специалистов в области информационной безопасности. Сетевые администраторы не являются и никогда не будут этими специалистами. У них хватает ежедневных проблем, на которые уходят все силы и время. Надежды на разработчиков программного обеспечения тоже маловероятны. У них хватает проблем с сопровождением разработанных продуктов и постоянной их адаптацией под изменяющиеся требования заказчиков. Кроме того, системные администраторы и разработчики в свою очередь являются фактором риска и на сегодняшний день достаточно большим.

В-четвертых. К кому обратиться, если вы, наконец, решили, что вашей компании или организации необходимы консалтинговые услуги в области информационной безопасности; кого предпочесть, чтобы ваш заказ был качественно выполнен, а итогом работы был не только отчет в виде списка уязвимых мест, полученного автоматическими сканерами безопасности, наподобие SATAN?

Мы можем порекомендовать обращаться к услугам фирм, которые специализируются в области информационной безопасности и обязательно (!) имеют специальные лицензии Департамента специальных телекоммуникационных систем и защиты информации.

Кроме того, вы можете обращаться непосредственно к автору данной статьи за консультациями и помощью. Телефон (044) 534 2540, e-mail: Byuriy@bartec.kiev.ua.

Литература: 1. Computer Security Issues & Trends / 2001 CSI/FBI Computer Crime and Security Survey – Vol. V11, No. 1

УДК 681.3:34

ОСНОВИ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ДЕРЖАВНИХ ОРГАНІВ УКРАЇНИ

Ігор Близнюк, Вячеслав Шорошев
НДІ НАВС України

Анотація: **Розглядаються основи нормативного та правового забезпечення захисту інформації в комп'ютерних системах, їх регулятивні та захисні функції, напрямки, об'єкти і суб'єкти, правовий статус, режим та рівні.**

Summary: **In the article the objects and subjects, directions, legal status, mode and levels are considered a fundamentals of normative and legal maintenance of protection of the information in computer systems, them regulations and protective functions.**

Ключові слова: **Нормативне та правове забезпечення, правовий статус, рівні правового режиму.**

Одним із завдань правового забезпечення державної політики в сфері інформатизації та формування інформаційних ресурсів є створення нормативно-правових засад, включаючи питання підготовки, введення і коригування нормативно-правових актів, які забезпечують функціонування інформації як продукту суспільного виробництва, регулюють доступ до такої інформації, визначають правила обертання інформаційних потоків у відомчій мережі та інше. Як свідчить досягнутий досвід забезпечення безпеки інформації в комп'ютерних системах [1], успішність захисту інформації в комп'ютерних системах залежить від нормативно-правового забезпечення (до 60%), апаратно-програмного забезпечення (до 30%) та організаційних заходів (до 10%). Ця пріоритетність поступово, зі зростанням правової та технічної дисципліни персоналу комп'ютерних систем та досвіду їх експлуатації, перерозподіляється до апаратно-програмного забезпечення та оперативних організаційних заходів забезпечення безпеки.

Основними **напрямками** правового забезпечення захисту інформації в комп'ютерних системах (КС) України є:

- захист інформації в інтересах її власників;
- захист інформації в інтересах держави, юридичних і фізичних осіб, що є споживачами цієї інформації;
- захист інформації в інтересах юридичних і фізичних осіб, про яких накопичується, зберігається, опрацьовується і передається ця інформація.