УДК 004.056

Н. А. Мазов, А. В. Ревнивых, А. М. Федотов

Институт нефтегазовой геологии и геофизики СО РАН
пр. Акад. Коптюга, 3, Новосибирск, 630090, Россия

Институт вычислительных технологий СО РАН
пр. Акад. Лаврентьева, 6, Новосибирск, 630090, Россия

Новосибирский государственный университет
ул. Пирогова, 2, Новосибирск, 630090, Россия

E-mail: alexchr@mail.ru, fedotov@nsc.ru

КЛАССИФИКАЦИЯ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ [*]

В работе описывается подход к анализу рисков информационной безопасности в корпоративной системе. Под информационной безопасностью понимается защищенность информационных ресурсов (информационных систем) и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информационных ресурсов.

Ключевые слова: информационная безопасность, риски, классификация угроз, доступ к информации, распределенные информационные ресурсы.

Введение

Корпоративные информационно-телекоммуникационные системы предназначены для получения определенных информационных услуг. Если по тем или иным причинам получение этих услуг пользователями становится невозможным, это наносит ущерб всем субъектам информационных отношений. Поэтому важнейшим элементом информационной безопасности является доступность тех или иных сервисов информационных систем.

Исходя из этого тезиса можно сформулировать основные задачи обеспечения информационной безопасности [1]:

- создание механизмов своевременного выявления, прогнозирования, локализации и оперативного реагирования на угрозы безопасности и проявления негативных тенденций в использовании информационных ресурсов и систем;
- создание эффективных регламентирующих документов обеспечения информационной безопасности;
- анализ и оценка рисков нарушения информационной безопасности;
- создание технологической и материально-технической базы информационной безопасности;
- обеспечение правовой защиты субъектов информационных отношений;
- сохранение и эффективное использование информационных ресурсов;
- координация деятельности субъектов информационного обмена в обеспечении информационной безопасности;
- унификация требований к обеспечению информационной безопасности;

[*] Работа выполнена при частичной поддержке РФФИ: проекты № 08-07-00229, 09-07-00277, 10-07-00302, Президентской программы «Ведущие научные школы РФ» (грант № НШ 6068.2010.9) и интеграционных проектов СО РАН.

© Н. А. Мазов, А. В. Ревнивых, А. М. Федотов, 2011

- обеспечение надежного функционирования информационных систем и предоставляемых ими услуг.

Отметим, что проблемы информационной безопасности затрагивают все уровни научно-технологического обеспечения – от теоретических основ и международных стандартов до оперативного администрирования.

Одним из важнейших аспектов информационной безопасности является задача анализа и управления рисками ее нарушения. Эта задача является неотъемлемой частью управления корпоративной информационной инфраструктурой и одним из важнейших условий обеспечения ее качества.

По определению, данному в рекомендациях ГОСТ ISO 15408 [2], риск –это вероятность реализации угрозы информационной безопасности. В классическом представлении оценка рисков включает оценку угроз, уязвимостей и наносимого ущерба. В этой связи возникают следующие вопросы.

Можно ли идентифицировать риски, влияющие на успешное функционирование инфраструктуры, на ранних стадиях проявления?

Можно ли обеспечить корректные и надежные результаты с теми ресурсами, которые выделены для поддержки инфраструктуры?

Какие части системы представляют собой наибольший риск для обеспечения требуемой функциональности, работоспособности и надежности?

Для возможного ответа на эти вопросы в данной статье предпринята попытка систематизировать риски.

Риски нарушения информационной безопасности

Пожалуй, основная причина возможной серьезности последствий нарушения информационной безопасности заключается в глобальности распространения информационных технологий и систем.

История человеческой цивилизации свидетельствует о том, что люди испокон веков стремились сделать физический и умственный труд более удобным. Апогеем воплощения человеческого желания «лучшей жизни» становятся результаты научно-технической революции. Следствия этой революции многократно предсказывали писатели-фантасты, и в настоящее время можно констатировать справедливость многих их умозаключений.

Трудно найти пример какой-либо области человеческой жизни, который бы до сих пор так или иначе не был бы связан с информационными системами. Электронными становятся книги, учебники, СМИ, тренажеры, деньги, документы (в том числе удостоверяющие личность человека, а также дающие ему те или иные полномочия в обществе), билеты на проезд в транспортных средствах и на поход в кино… Электроникой испещрены транспортные средства (автомобили, корабли, самолеты, поезда), музыкальные инструменты, бытовая техника (складывается ощущение, что компьютер в домашних условиях уже тоже относится к бытовой технике). Отдельного упоминания достойны средства связи, которые стремительно компьютеризируются. Буквально за 10–15 лет возникло несколько совершенно новых технологий средств связи (Instant Messengers (1996), VoIP (2003), социальные сети и т. д.). Да и мобильные телефоны стремительно превращаются в мобильные компьютеры.

Важно, что меняется контекст способа жизни людей. И основные причины этого, по всей видимости, постоянное ускорение обмена информацией и вообще увеличение объема информационных потоков, которые ежесуточно вынужден поглощать человек.

Таким образом, поддержание информационной безопасности, с одной стороны, становится очень важным аспектом буквально для любого человека, а с другой стороны, является очень уязвимым. За любым современным человеком, проживающим в цивилизованной стране, буквально можно следить с помощью его же бытовой электроники, которую он ежедневно использует. Мобильные телефоны, имеющие номер SIM-карты и IMEI, по которым можно однозначно установить, на кого зарегистрирован телефон и его местонахождение; GPS-навигаторы, которые отсылают свое местонахождение в систему, образуемую спутниковой группировкой; кредитные и «скидочные» карточки; серийные номера и программно-аппаратные конфигурации компьютеров (в том числе мобильных), которые используют для

эксплуатации сервисов сети Internet. Уже не говоря о IP-адресе шлюза, через который пользователи подключаются к Internet. К тому же огромное количество пользователей собирают «социальные сети», в которых люди сами же по собственной воле (хотя, вероятно, не всегда предполагая все возможные последствия этого) выкладывают свои персональные данные. Немаловажно и неистребимое желание людей отправлять персональную информацию через средства социальных сетей, электронной почты, сервисов мгновенного обмена сообщениями, мобильной связи (SMS, MMS), файлообменные сервисы и т. д.

Люди не задумываются о том, что даже по последовательности запросов к распространенным поисковым системам их личность и интересы уже можно идентифицировать, имея доступ к базе истории поисковых запросов.

История запросов к поисковым системам с определенных IP-адресов стала достоянием общественности благодаря научно-исследовательским работам, проводившимся учеными, с целью усовершенствования поисковых алгоритмов.

Средства массовой информации, писатели и кинематографисты дополнительно усугубляют ситуацию, связанную с и без того невысоким уровнем знаний пользователей в области информационной безопасности. Например, во время художественного фильма показывается, как герой ломает и выбрасывает SIM-карту, а затем вставляет в тот же телефонный аппарат новую и почему-то чувствует себя в полной безопасности от прослушки и пеленгования местонахождения, снова включая мобильный телефон с тем же IMEI-идентификатором.

Анализируя работы, посвященные проблемам информационной безопасности (см., например, [3–5]), можно отметить, что понятие информационной безопасности (ИБ) трактуется очень широко и включает огромное количество аспектов. При этом степень исследованности различных аспектов сильно отличается.

Работы можно классифицировать по применяемому авторами подходу к выбору объектов исследований.

- Узкоспециализированные исследования в области какого-то конкретного аспекта ИБ. К данной категории относится изучение уязвимостей конкретной операционной системы или прикладной программы либо же какой-то технологии и выработка рекомендаций по снижению вероятности нарушения режима безопасности (а порой и наоборот – инструкции по эффективному использованию имеющихся уязвимостей). Сюда же относятся работы, связанные, например, с вредоносным программным обеспечением или же, наоборот, антивирусными программами; различного рода сетевыми атаками; надежностью работы оборудования и программного обеспечения информационных систем; криптографией и т. д.
- Попытки исследований ИБ в целом. В основном сводятся к изучению нескольких аспектов ИБ в рамках одного исследования. Представляется, что объять все возможные направления исследований в одной работе невозможно. При этом авторы классифицируют аспекты ИБ, дают свои варианты определений термину ИБ, в чем, безусловно, есть необходимость и ценность. Кроме того, сюда же отнесем стандарты ИБ (хотя и они на практике всегда относятся к необходимой для субъекта (организации, государства) группе аспектов).

Подавляющее большинство работ в области ИБ относится к первой категории. Недостатком такого подхода является невозможность построения всех имеющихся причинно-следственных взаимосвязей, влияющих в конечном счете на выбранный к рассмотрению аспект ИБ. Немаловажно, что это ведет к концептуальности и стереотипности выводов по проведенным исследованиям: автор приходит к определенному мнению, которое основано на ограниченном количестве экспериментов и критериев, учитывавшихся при этих экспериментах и логических выкладках.

К сожалению, очень мало исследований проводилось в области анализа рисков нарушения ИБ. Здесь речь идет как об изучении вероятности нарушения режима ИБ, так и о прогнозировании последствий такого рода инцидентов. При этом представляется, что данное направление исследований обладает чрезвычайной важностью. Только анализируя и моделируя риски нарушения ИБ, можно эффективно задавать весовые коэффициенты различных аспектов ИБ как в общем, так и в отдельно рассматриваемой информационной системе.

С точки зрения анализа рисков следует выделить монографию [6], где подробно рассмотрены возможные постановки задач анализа информационных рисков и управления ими при организации режима информационной безопасности. Рассмотрена международная концепция

обеспечения информационной безопасности, а также различные подходы и рекомендации по решению задач анализа рисков и управления ими. Дан обзор основных стандартов в области защиты информации и управления рисками: ISO 17799, ISO 15408, BSI, NIST, MITRE. Показана взаимосвязь задач анализа защищенности и обнаружения вторжений с задачей управления рисками. Предложены технологии оценки эффективности обеспечения информационной безопасности. При этом в данном труде, как и в других найденных источниках, отсутствует подходы [1] к классификации «рисков», связанных с нарушениями ИБ.

Классификация рисков нарушения информационной безопасности

Разработка классификации рисков нарушения информационной безопасности представляется важной задачей для их эффективного изучения и разработки технических и организационных мер для учета рисков, их прогнозирования, управления рисками, оценки эффективности этих мер с точки зрения отношения затрат к надежности.

Однако до сих пор попытки использования классификаций для описания по возможности большего количества угроз показали, что во многих случаях реальные угрозы либо не подходили ни под один из классификационных признаков, либо, наоборот, удовлетворяли нескольким.

Основная цель создания классификации угроз – наиболее полная, детальная классификация, которая описывает все существующие угрозы информационной безопасности, по которой каждая из угроз попадает только под один классификационный признак и которая, таким образом, наиболее применима для анализа рисков реальных информационных систем. Отметим, что при классифицировании в первую очередь необходимо определиться с возможными *аспектами* и *критериями* ИБ.

По-видимому, наиболее правильную классификацию даст подход, опирающийся на составляющие «рисков» информационной безопасности.

Для управления рисками требуется идентифицировать возможные угрозы. Таковыми могут являться, например, наводнение, отключение электропитания или атаки злоумышленников с последствиями разной степени тяжести.

Вторая задача состоит в построении модели нарушения.

Как отмечается в ГОСТ ISO 15408 [2], понятие «риска» является следствием взаимного соотношения понятий «актив», «уязвимость», «угроза» и «ущерб»:

- активы – ключевые компоненты инфраструктуры и значимая для собственника информация, обрабатываемая в информационной системе, имеющая определенную ценность [2];
- угроза – потенциальная возможность нанесения ущерба каким-либо заранее известным способом;
- уязвимость – слабое место в средствах защиты, вызванная ошибками или несовершенством в процедурах, проекте, реализации, которую «угроза» может преодолеть;
- ущерб – затраты на восстановление системы в исходное состояние после возможного инцидента ИБ.

Под риском подразумевается сочетание вероятности нанесения ущерба путем преодоления системы защиты с использованием уязвимостей и тяжести этого ущерба.

Минимизация рисков осуществляется с помощью разработки схемы поведения, так называемой «политики безопасности» и управления ею. Управление работами по реализации политики безопасности – это и есть управление рисками.

Таким образом, анализ понятия «риск нарушения информационной безопасности» должен основываться на анализе «причин нарушения ИБ» и «последствий нарушения ИБ».

---

[1] Основное внимание авторы уделяют классификации угроз и анализу уязвимостей нарушений ИБ.

[2] Стандарт ГОСТ ISO 17799, подробно описывающий процедуры системы управления ИБ, выделяет следующие виды активов: информационные ресурсы (базы и файлы данных, контракты и соглашения, системная документация, научно-исследовательская информация, документация, обучающие материалы и пр.); программное обеспечение; материальные активы (компьютерное оборудование, средства телекоммуникаций и пр.); сервисы (сервисы телекоммуникаций, системы обеспечения жизнедеятельности и др.); сотрудники компании, их квалификация и опыт; нематериальные ресурсы (репутация и имидж компании).

Рассмотрим далее основные аспекты информационной безопасности: доступность, целостность, конфиденциальность.

Доступность. Под доступностью информации будем понимать возможность доступа субъекта к данным по запросу в любое предусмотренное расписанием работы системы время. При этом доступ к информации имеет смысл разделить на несколько этапов:

- возможность для субъекта отправить запрос на определенные данные в информационную систему (зависит от работоспособности интерфейса системы, через который она принимает такие запросы, а также от исправности и загруженности канала связи между субъектом и сервером);
- генерирование системой ответа на запрос в течение промежутка времени, не превышающего значение тайм-аута (зависит от работоспособности системы, а также от ее загруженности обработкой других запросов или иной работой);
- возможность доставить ответ информационной системы до субъекта в течение времени, не превышающего тайм-аут (зависит от работоспособности интерфейса системы, через который она отправляет ответы на запросы, а также от исправности и загруженности канала связи между субъектом и сервером).

Итак, возможность получения данных по запросу зависит от работоспособности и загруженности канала связи между пользователем и интерфейсом информационной системы и от работоспособности и загруженности самой информационной системы.

Технические причины нарушения канала связи между пользователем и интерфейсом системы могут быть самыми различными – от банальных неисправностей оборудования и сбоев программного обеспечения до успешных реализаций атак на отказ в обслуживании (PING-flooding, SYN-flooding, DDOS).

При этом отражение атак на отказ в обслуживании затруднено в связи с особенностями наиболее распространенного в локальных сетях и Internet программного сетевого протокола транспортного уровня IPv4.

Риск нарушения работоспособности информационной системы, содержащей запрашиваемую пользователем информацию, зависит от надежности совокупности аппаратных и программных компонентов, составляющих систему, а также от адекватности оператора, управляющего их работой. Нарушения доступности возникают из-за несоблюдения требований стандартов на этапе проектирования, производства или эксплуатации системы.

Целостность. Под целостностью будем понимать актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения или удаления.

Риск нарушения целостности информации обеспечивается следующими факторами:

- вероятностью отказа оборудования и программного обеспечения информационной системы, так как нарушение актуальности и непротиворечивости данных может произойти в результате сбоев при их работе;
- степенью продуманности алгоритмов и надежностью аутентификации пользователей системы, имеющих право на редактирование хранящихся в ней данных;
- вероятностью наличия в программном обеспечении недокументированных возможностей;
- несоблюдением требований стандартов на этапе проектирования, производства или эксплуатации системы;
- несовершенством организационной структуры ИС. Например, необходимость частой перенастройки системы или ее отдельных частей чревата нарушением целостности хранящихся и обрабатываемых в ней данных, а также дополнительными затратами;
- человеческим фактором. Например, вероятностью социальной инженерии по отношению к лицам, имеющим доступ к редактированию данных, хранящихся в системе. Инсайдерские угрозы.

Конфиденциальность. Под конфиденциальностью будем понимать защищенность информации от несанкционированного доступа на чтение.

Риск нарушения конфиденциальности информации обеспечивается следующими факторами:

- степенью продуманности алгоритмов и надежностью аутентификации пользователей системы, имеющих право на доступ к хранящимся в ней данным;
- вероятностью наличия в программном обеспечении недокументированных возможностей;
- несоблюдением требований стандартов на этапе проектирования, производства или эксплуатации системы;
- несовершенством организационной структуры ИС. Например, необходимость частой перенастройки системы или ее отдельных частей чревата нарушением конфиденциальности хранящихся и обрабатываемых в ней данных, а также дополнительными затратами;
- человеческим фактором. Например, вероятностью социальной инженерии по отношению к лицам, имеющим доступ к системе. Инсайдерские угрозы

Причины нарушения ИБ

Причины нарушения информационной безопасности, в первую очередь, вызваны реализацией той или иной угрозы. Как уже отмечалось, возможности реализации угроз зависят от «модели» нарушения. Нарушения ИБ могут быть вызваны двумя причинами: либо действиями «злоумышленников», либо действиями «обстоятельств».

По всей видимости имеет смысл строить две системы классификации рисков, основанных на «модели» нарушения.

С учетом классификации угроз анализ и классификацию рисков следует вести по характеру угрозы информационной безопасности, которые можно разделить на технологические и организационные и которые могут составить верхний уровень классификации:

Технологические. Связаны с оборудованием, программным обеспечением, их задачами, способами проектирования и разработки, дальнейшей сборки и эксплуатации.

Организационные. Связаны с непредсказуемостью деятельности персонала, эксплуатирующего и обслуживающего информационную систему.

Классификация причин нарушения информационной безопасности разделяется по характеру угрозы, видам воздействия, причине и объекту угрозы.

Технологические причины нарушения ИБ напрямую связаны с жизненным циклом информационных систем [7].

Жизненный цикл любой информационной системы состоит из последовательности нескольких этапов

1. Идея о создании информационной системы для облегчения умственной или физической работы.
2. Разработка технического задания.
3. Проектирование системы.
4. Утверждение проекта.
5. Производство системы.
6. Тестовая эксплуатация.
7. Устранение недостатков проекта или производства.
8. Эксплуатация (обычно это самый длительный этап).
9. Вывод из эксплуатации.
10. Утилизация.

Можно обратить внимание на то, что ни один этап не обходится без человека. Неизбежны риски нарушения надежности и безопасности при эксплуатации информационных систем, задуманных, созданных и эксплуатируемых людьми и для людей.

При этом тема о различиях людских типов темперамента (холерики, сангвиники, флегматики и меланхолики), основных каналов восприятия информации (визуалы, аудиалы, кинестетики и дигиталы) и психотипах (компульсивный, шизоидный, истероидный и депрессивный) неисчерпаема. Работоспособность, внимание, мотивация людей зависит от колоссального количества всевозможных параметров. При этом современные информационные системы неизбежно являются результатом работы множества людей, плоды труда которых приходится увязывать в рамках одного конечного продукта.

Поскольку алгоритмы программных модулей к одной и той же информационной системе разрабатывают несколько программистов (а то и команд разработчиков), то наивно было бы предполагать, что эти модули будут идеально совмещены друг с другом в конечном продукте. Особенно это проявляется в случаях, когда при проектировании система изначально не снабжалась нормативной документацией либо же нарушались требования соответствующих стандартов.

В некоторых информационных системах в силу разных причин возникают возможности несанкционированного входа в систему в обход штатных средств аутентификации пользователей. Часто это происходит из-за того, что при разработке ранних версий системы делаются закладки для ее дальнейшего совершенствования. Потом же эти закладки не реализуются, но при этом в коде проекта остаются. Кроме того, можно предположить, что иногда разработчики специально оставляют в системе «черный вход» для себя, о способе использования которого нередко узнают и злоумышленники.

Кроме того, неидеальное совмещение разных модулей системы (упомянутое выше) тоже может предоставить аналогичные возможности несанкционированного подключения.

Особую роль в технологических причинах играют «недокументированные возможности программного обеспечения».

Риск использования злоумышленниками, а также случайных проявлений так называемых недокументированных возможностей программного обеспечения появляются в силу разных причин.

- Сложность и объемность современного программного обеспечения. Кроме сложности и объемности, сюда же примыкает и тот факт, что программы в настоящее время уже невозможно разрабатывать силами одного человека: так или иначе приходится увязывать в рамках одного проекта результаты труда одной или даже нескольких команд разработчиков. Таким образом, в абсолютно любой программе содержится множество логических ошибок, которые могут проявляться самым непредсказуемым образом в неожиданные моменты. Кроме того, очень сложно контролировать возможность добавления разработчиками к программному коду различного рода «закладок».
- Однотипность используемых в качестве хост-платформы операционных систем. В мире создано не очень большое количество разнообразных операционных систем, поэтому, изучив особенности большинства из них, злоумышленник может определить тип используемой в интересующем его объекте операционной системы и воспользоваться ее уязвимостями, которые можно считать недокументированными возможностями.
- Подавляющее количество сетевого программного обеспечения написано с использованием языков C/C++, особенность которых в том, что проекты, написанные на них, так или иначе подвержены атакам на срыв стэка и переполнение буфера. Даже запрос на ввод имени пользователя и пароля может стать мишенью для атаки на доступ к информационной системе. Хотя здесь необходимо отметить, что для программного обеспечения, авторы которого соблюдали стандарты, вероятность успешной атаки на срыв стека мала. Возможность практической реализации такой атаки очень маловероятна для продуктов, где обеспечивается модульность компонентов. Например, модуль аутентификации, запрашивающий имя пользователя и его пароль, должен быть отдельным от основной системы компонентом.

Организационные причины нарушения ИБ

- *Уровень компетентности разработчиков.* Функциональность и сложность информационных систем непрерывно (и очень быстро) возрастают. При этом, как уже отмечалось, даже среди разработчиков современных ИС нет ни одного человека, который бы полностью представлял, как работает система. Во-первых, потому что он не был единственным разработчиком данной системы, а во-вторых, потому что свою систему он неизбежно разрабатывал на основе каких-то (созданных ранее и другими людьми) модулей (например, писал программное обеспечение с помощью существующего языка программирования высокого уровня для уже готовой операционной системы, работающей на имеющемся оборудовании).
- *Уровень компетентности пользователей.* Пользователям приходится ежедневно разбираться с большим количеством разнородных информационных систем. Возникает необходимость еще и увязывать различные системы между собой. При этом нет никаких курсов повышения квалификации, на которых людей учили бы пользоваться всеми возможными

информационными системами сразу. И уж в последнюю очередь пользователи заботятся о безопасности: «Лишь бы работало!». Дополнительно стараются и разработчики, выпуская все новые и новые версии своих информационных систем (или их частей), например, каждые полгода. Только пользователи научились более-менее уверенно управляться с системой, как выходит ее новая версия, с которой опять нужно разбираться, в которой исправлены ошибки, к которым уже привыкли и адаптировались, и добавлены новые, к которым привыкать и адаптироваться еще только предстоит.

• *Человеческий фактор.* Людям свойственно ошибаться. Случайные и неосознанные действия пользователей информационных систем становятся причиной нарушения ИБ.

Классификационная схема причин нарушения ИБ

Приведем логическое описание представленной схемы.

1. Угрозы технологического характера. Технологические угрозы информационной безопасности по виду воздействия делятся на физические и программные.

• Физические. Причинами реализации физических угроз могут быть:

– действия нарушителя (человека). Независимо от причины физические угрозы воздействуют:

▪ на ресурс;
▪ на канал связи.

– форс-мажорные обстоятельства;
– отказ оборудования и внутренних систем жизнеобеспечения.

• Программные (логические). По причине воздействия программные угрозы можно разделить на:

– угрозы, исходящие от локального нарушителя.

Объектом локального нарушителя может быть только ресурс. В свою очередь, на ресурсе локальный нарушитель может реализовать угрозы, направленные:

▪ на операционную систему;
▪ на прикладное программное обеспечение;
▪ на информацию.

– угрозы, исходящие от удаленного нарушителя, которые могут воздействовать:

▪ на ресурс;

При доступе к ресурсу удаленный нарушитель может воздействовать:

o на операционную систему;
o на сетевые службы;
o на информацию;

▪ на канал связи.

При воздействии на канал связи удаленный нарушитель может реализовать угрозы, направленные:

o на сетевое оборудование;
o на протоколы связи.

2. Угрозы организационного характера.

Организационные угрозы по характеру воздействия можно разделить на:

• воздействие на персонал;

Воздействие на персонал может быть:

– физическим;

Как физическое, так и психологическое воздействие на персонал направлено на сотрудников компании с целью:

▪ получения информации;
▪ нарушения непрерывности ведения бизнеса;

– психологическим;

• действия персонала.

Причинами действий персонала, способных вызвать угрозы информационной безопасности, могут быть:

– умышленные действия;

Угрозы, вызванные умышленными действиями персонала, могут быть направлены:

- на информацию;
- на непрерывность ведения бизнеса.

– неумышленные действия.

Угрозы, вызванные неумышленными действиями персонала, могут быть направлены:

- на информацию;
- на непрерывность ведения бизнеса.

Ниже приведена классификационная схема, представленная в виде рубрикатора. Такая схема позволяет при необходимости расширять понятия, находящиеся в узлах дерева рубрикатора.

0. Угрозы информационной безопасности
0.1. Угрозы технологического характера
0.1.1. Физические
0.1.1.1. Действия нарушителя (человека)
0.1.1.1.1. На ресурс
0.1.1.1.2. На канал связи
0.1.1.2. Форс-мажорные обстоятельства
0.1.1.3. Отказ оборудования и внутренних систем жизнеобеспечения
0.1.2. Программные (логические)
0.1.2.1. Угрозы, исходящие от локального нарушителя
0.1.2.1.1. На операционную систему
0.1.2.1.2. На прикладное программное обеспечение
0.1.2.1.3. На информацию
0.1.2.2. Угрозы, исходящие от удаленного нарушителя
0.1.2.2.1. На ресурс
0.1.2.2.1.1. На операционную систему
0.1.2.2.1.2. На сетевые службы
0.1.2.2.1.3. На информацию
0.1.2.2.2. На канал связи
0.1.2.2.2.1. На сетевое оборудование
0.1.2.2.2.2. На протоколы связи
0.2. Угрозы организационного характера
0.2.1. Воздействие на персонал
0.2.1.1. Физические
0.2.1.1.1. Получения информации
0.2.1.1.2. Нарушения непрерывности ведения бизнеса
0.2.1.2. Психологические
0.2.2. Действия персонала
0.2.2.1. Умышленные действия
0.2.2.1.1. На информацию
0.2.2.1.2. На непрерывность ведения бизнеса
0.2.2.2. Неумышленные действия
0.2.2.2.1. На информацию
0.2.2.2.2. На непрерывность ведения бизнеса

Последствия нарушения ИБ

При классифицировании последствий нарушения режима ИБ имеет смысл начать с глобальности распространения и глубины внедрения информационных технологий в целом. Исходя из этого становится очевидным, что в качестве пострадавшего субъекта может выступать как конкретная личность или небольшая группа людей (например, семья), так и организация или целое государство. Также имеет смысл учитывать, что одно и то же следствие не может быть полностью вызвано только какой-то одной конкретной причиной – причин одного и того же события множество. Кроме того, при классифицировании будем обра-

щать внимание на относительность оценок одного и того же события разными субъектами (для владельца банковского счета его взлом – негативное событие, а для взломщика – позитивное, по крайней мере, в недалекой перспективе). Чтобы избежать неоднозначности трактовок, классифицировать возможные последствия нарушения режима ИБ будем исходя из предполагаемой их оценки пострадавшим субъектом. Однако при таком подходе необходимо учитывать, что одно и то же нарушение ИБ может иметь негативные последствия не только для того субъекта, со стороны которого мы его изучаем, но и для других субъектов (например, государству вряд ли выгодно, если один или несколько его граждан обеднеют).

Представляется необходимым ввести дополнительный критерий классификации - степень нанесенного инцидентом вреда, а также ограничение по дальности перспективы изучения последствий (например, для обедневших граждан этот факт может стать вдохновляющим на новые свершения в жизни, которые сделают их еще успешнее).

Заключение

В данной работе мы привели начальный уровень классификации рисков нарушения информационной безопасности. Риск определяется вероятностью причинения ущерба и величиной ущерба, наносимого организации, в случае осуществления угрозы безопасности.

На основе относительно полной системы классификации можно оценить как ущерб, вызванный нарушением ИБ, так и затраты на защиту от угроз нарушения ИБ.

Анализ рисков позволит спланировать мероприятия по определению того, какие ресурсы и от каких угроз надо защищать, а также в какой степени те или иные ресурсы нуждаются в защите.

Список литературы

1. *Федотов А. М.* Информационная безопасность в корпоративной сети // Проблемы безопасности и чрезвычайных ситуаций / ВИНИТИ. М.: ВИНИТИ, 2008. № 2. С. 88–101.

2. ГОСТ Р ИСО/МЭК 15408-1(2,3) – 2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 1–3.

3. *Галатенко В. А.* Основы информационной безопасности. М., 2004.

4. *Ярочкин В. И.* Информационная безопасность. М.: Академический проект; Гаудеамус, 2004.

5. *Белов Е. Б., Лось В. П.и др.* Основы информационной безопасности. М.: Горячая линия, 2006.

6. *Петренко С. А., Симонов С. В.* Управление информационными рисками. Экономически оправданная безопасность. М.: ДМКпресс, 2004.

7. *Шокин Ю. И., Федотов А. М., Барахнин В. Б.* Проблемы поиска информации. Новосибирск: Наука, 2010. 198 с.

8. ISO/IEC14252-1996(ANSI/IEEEStd1003.0-1995) Information technology – Guide to the POSIX Open Systems Environment(OSE).

Материал поступил в редколлегию 29.04.2011

N. A. Mazov, A. V. Revnivykh, A. M. Fedotov

ANALYSIS OF INFORMATION SECURITY RISKS

Thispaperdescribesanapproachtotheanalysisofinformationsecurityrisksinthecorporatesys-
risksinthecorporatesys-
tem.UndertheInformationSecurityreferstoprotectionofinformationresources(informationsystems)andsupportinginfrastructu
refromaccidentalordeliberateexposuretonaturalorartificial,withthepotentialdamagetotheownersorusersofinformationresourc
es.

Keywords: information security risks, access to information, distributed information resources.