

**НЕГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «РОС-
СИЙСКАЯ АКАДЕМИЯ АДВОКАТУРЫ И НОТАРИАТА»**

Реферат

на тему: «Информационная безопасность и управление
рисками»

Выполнил:
Магистрант 2 курса
Рубинская В. Г.

Проверил:

Москва, 2018

Содержание

Введение.....	1
Раздел 1. Понятие информационной безопасности.....	2
Раздел 2. Управление рисками.....	7
Раздел 3. Подготовительные и основные этапы управления рисками...	10
Заключение.....	16
Список использованных источников	

Введение

Современное развитие мировой экономики характеризуется все большей зависимостью рынка от значительного объема информационных потоков. Актуальность проблем, связанных с защитой потоков данных и обеспечением информационной безопасности их обработки и передачи, все более усиливается. Проблема защиты информации является многоплановой и комплексной. Современное развитие электроники, технических средств обработки, хранения и защиты информации происходит интенсивно. Одновременно совершенствуются и средства несанкционированного доступа и использования, как на программном, так и на программно-аппаратном уровне.

Словосочетание «информационная безопасность» в разных контекстах может иметь различный смысл. В Доктрине информационной безопасности Российской Федерации термин "информационная безопасность" используется в широком смысле. Имеется в виду состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

В Законе РФ "Об участии в международном информационном обмене" (закон утратил силу, в настоящее время действует "Об информации, информационных технологиях и о защите информации") информационная безопасность определяется аналогичным образом – как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Раздел 1. Понятие информационной безопасности

Под информационной безопасностью понимается защищенность информации и поддерживающей ее инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или поддерживающей инфраструктуре.

Информационная безопасность организации - состояние защищенности информационной среды организации, обеспечивающее её формирование, использование и развитие.

В современном социуме информационная сфера имеет две составляющие: информационно-техническую (искусственно созданный человеком мир техники, технологий и т.п.) и информационно-психологическую (естественный мир живой природы, включающий и самого человека). Соответственно, в общем случае информационную безопасность общества (государства) можно представить двумя составными частями: информационно-технической безопасностью и информационно-психологической (психофизической) безопасностью¹

В качестве стандартной модели безопасности часто приводят модель из трёх категорий:

Конфиденциальность - состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право;

Целостность - избежание несанкционированной модификации информации;

Доступность - избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.

Выделяют и другие не всегда обязательные категории модели безопасности:

неотказуемость или апеллируемость - невозможность отказа от

¹ Галатенко, В.А. Основы информационной безопасности. Интернет-университет информационных технологий . ИНТУИТ.ру, 2008. – 22 с.

авторства;

подотчётность - обеспечение идентификации субъекта доступа и регистрации его достоверность - свойство соответствия предусмотренному поведению или результату;

аутентичность или подлинность - свойство, гарантирующее, что субъект или ресурс идентичны заявленным².

Действия, которые могут нанести ущерб информационной безопасности организации, можно разделить на несколько категорий:

1. Действия, осуществляемые авторизованными пользователями. В эту категорию попадают: целенаправленная кража или уничтожение данных на рабочей станции или сервере; повреждение данных пользователей в результате неосторожных действий.

2. «Электронные» методы воздействия, осуществляемые хакерами. Под хакерами понимаются люди, занимающиеся компьютерными преступлениями как профессионально (в том числе в рамках конкурентной борьбы), так и просто из любопытства. К таким методам относятся: несанкционированное проникновение в компьютерные сети; DOS_атаки.

Целью несанкционированного проникновения извне в сеть предприятия может быть нанесение вреда (уничтожения данных), кража конфиденциальной информации и использование ее в незаконных целях, использование сетевой инфраструктуры для организации атак на узлы третьих фирм, кража средств со счетов и т.п.

Атака типа DOS (сокр. от Denial of Service - «отказ в обслуживании») - это внешняя атака на узлы сети предприятия, отвечающие за ее безопасную и эффективную работу (файловые, почтовые сервера). Злоумышленники организуют массированную отправку пакетов данных на эти узлы, чтобы вызвать их перегрузку и, в итоге, на какое-то время вывести их из строя. Это, как правило, влечет за собой нарушения в бизнес-процессах компании-

² Галатенко, В.А. Стандарты информационной безопасности. Интернет-университет информационных технологий. ИНТУИТ.ру, 2005. – 39 с.

жертвы, потерю клиентов, ущерб репутации и т.п.

3. Компьютерные вирусы. Отдельная категория электронных методов воздействия - компьютерные вирусы и другие вредоносные программы. Они представляют собой реальную опасность для современного бизнеса, широко использующего компьютерные сети, интернет и электронную почту. Проникновение вируса на узлы корпоративной сети может привести к нарушению их функционирования, потерям рабочего времени, утрате данных, краже конфиденциальной информации и даже прямым хищениям финансовых средств. Вирусная программа, проникшая в корпоративную сеть, может предоставить злоумышленникам частичный или полный контроль над деятельностью компании.

4. Спам. Всего за несколько лет спам из незначительного раздражающего фактора превратился в одну из серьезнейших угроз безопасности: электронная почта в последнее время стала главным каналом распространения вредоносных программ; спам отнимает массу времени на просмотр и последующее удаление сообщений, вызывает у сотрудников чувство психологического дискомфорта; как частные лица, так и организации становятся жертвами мошеннических схем, реализуемых спамерами; вместе со спамом нередко удаляется важная корреспонденция, что может привести к потере клиентов, срыву контрактов и другим неприятным последствиям; опасность потери корреспонденции особенно возрастает при использовании черных списков RBL и других «грубых» методов фильтрации спама.

5. «Естественные» угрозы. На информационную безопасность компании могут влиять разнообразные внешние факторы: причиной потери данных может стать неправильное хранение, кража компьютеров и носителей, форс-мажорные обстоятельства и т.д.³

Таким образом, в современных условиях наличие развитой системы информационной безопасности становится одним из важнейших условий

³ Щербаков, А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. М.: Книжный мир, 2009. – 194 с.

конкурентоспособности и даже жизнеспособности любой компании.

Раздел 2. Управление рисками

Информационная безопасность должна достигаться экономически оправданными мерами. В реферате описывается методика, позволяющая сопоставить возможные потери от нарушений ИБ со стоимостью защитных средств. Основные понятия Управление рисками рассматривается нами на административном уровне ИБ, поскольку только руководство организации способно выделить необходимые ресурсы, инициировать и контролировать выполнение соответствующих программ. Вообще говоря, управление рисками, равно как и выработка собственной политики безопасности, актуально только для тех организаций, информационные системы которых и/или обрабатываемые данные можно считать нестандартными. Обычную организацию вполне устроит типовой набор защитных мер, выбранный на основе представления о типичных рисках или вообще без всякого анализа рисков (особенно это верно с формальной точки зрения, в свете проанализированного нами ранее российского законодательства в области ИБ). Можно провести аналогию между индивидуальным строительством и получением квартиры в районе массовой застройки. В первом случае необходимо принять множество решений, оформить большое количество бумаг, во втором достаточно определиться лишь с несколькими параметрами. Более подробно данный аспект рассмотрен в статье Сергея Симонова "Анализ рисков, управления рисками" (Jet Info, 1999, 1). Использование информационных систем связано с определенной совокупностью рисков. Когда возможный ущерб неприемлемо велик, необходимо принять экономически оправданные меры защиты. Периодическая (пере)оценка рисков необходима для контроля эффективности деятельности в области безопасности и для учета изменений обстановки. С количественной точки зрения уровень риска является функцией вероятности реализации определенной угрозы (использующей некоторые уязвимые места), а также величины возможного ущерба.

Таким образом, суть мероприятий по управлению рисками состоит в том,

чтобы оценить их размер, выработать эффективные и экономичные меры снижения рисков, а затем убедиться, что риски заключены в приемлемые рамки (и остаются таковыми).

Следовательно, управление рисками включает в себя два вида деятельности, которые чередуются циклически:

(пере)оценка (измерение) рисков;

выбор эффективных и экономичных защитных средств (нейтрализация рисков).

По отношению к выявленным рискам возможны следующие действия:

ликвидация риска (например, за счет устранения причины);

уменьшение риска (например, за счет использования дополнительных защитных средств);

принятие риска (и выработка плана действия в соответствующих условиях);

переадресация риска (например, путем заключения страхового соглашения).

Процесс управления рисками можно разделить на следующие этапы:

- 1) Выбор анализируемых объектов и уровня детализации их рассмотрения.
- 2) Выбор методологии оценки рисков.
- 3) Идентификация активов.
- 4) Анализ угроз и их последствий, выявление уязвимых мест в защите.
- 5) Оценка рисков.
- 6) Выбор защитных мер.
- 7) Реализация и проверка выбранных мер.
- 8) Оценка остаточного риска.

Этапы 6 и 7 относятся к выбору защитных средств (нейтрализации рисков), остальные - к оценке рисков.

Уже перечисление этапов показывает, что управление рисками - процесс циклический. По существу, последний этап - это оператор конца цикла,

предписывающий вернуться к началу. Риски нужно контролировать постоянно, периодически проводя их переоценку. Отметим, что добросовестно выполненная и тщательно документированная первая оценка может существенно упростить последующую деятельность. Управление рисками, как и любую другую деятельность в области информационной безопасности, необходимо интегрировать в жизненный цикл ИС. Тогда эффект оказывается наибольшим, а затраты - минимальными. Ранее мы определили пять этапов жизненного цикла. Кратко опишем, что может дать управление рисками на каждом из них.

На этапе инициации известные риски следует учесть при выработке требований к системе вообще и средствам безопасности в частности. На этапе закупки (разработки) знание рисков поможет выбрать соответствующие архитектурные решения, которые играют ключевую роль в обеспечении безопасности. На этапе установки выявленные риски следует учитывать при конфигурировании, тестировании и проверке ранее сформулированных требований, а полный цикл управления рисками должен предшествовать внедрению системы в эксплуатацию.

На этапе эксплуатации управление рисками должно сопровождать все существенные изменения в системе. При выведении системы из эксплуатации управление рисками помогает убедиться в том, что миграция данных происходит безопасным образом.

Раздел 3. Подготовительные и основные этапы управления рисками

В этом разделе будут описаны первые три этапа процесса управления рисками. Выбор анализируемых объектов и уровня детализации их рассмотрения - первый шаг в оценке рисков. Для небольшой организации допустимо рассматривать всю информационную инфраструктуру; однако если организация крупная, всеобъемлющая оценка может потребовать неприемлемых затрат времени и сил. В таком случае следует сосредоточиться на наиболее важных сервисах, заранее соглашаясь с приближенностью итоговой оценки. Если важных сервисов все еще много, выбираются те из них, риски для которых заведомо велики или неизвестны. Мы уже указывали на целесообразность создания карты информационной системы организации. Для управления рисками подобная карта особенно важна, поскольку она наглядно показывает, какие сервисы выбраны для анализа, а какими пришлось пренебречь.

Если ИС меняется, а карта поддерживается в актуальном состоянии, то при переоценке рисков сразу станет ясно, какие новые или существенно изменившиеся сервисы нуждаются в рассмотрении. Вообще говоря, уязвимым является каждый компонент информационной системы - от сетевого кабеля, который могут прогрызть мыши, до базы данных, которая может быть разрушена из-за неумелых действий администратора. Как правило, в сферу анализа невозможно включить каждый винтик и каждый байт. Приходится останавливаться на некотором уровне детализации, опять-таки отдавая себе отчет в приближенности оценки. Для новых систем предпочтителен детальный анализ; старая система, подвергшаяся небольшим модификациям, может быть проанализирована более поверхностно. Очень важно выбрать разумную методологию оценки рисков. Целью оценки является получение ответа на два вопроса: приемлемы ли существующие риски, и если нет, то какие защитные средства стоит использовать. Значит, оценка должна быть количественной, допускающей сопоставление с заранее выбранными

границами допустимости и расходами на реализацию новых регуляторов безопасности.

Управление рисками - типичная оптимизационная задача, и существует довольно много программных продуктов, способных помочь в ее решении (иногда подобные продукты просто прилагаются к книгам по информационной безопасности). Принципиальная трудность, однако, состоит в неточности исходных данных. Можно, конечно, попытаться получить для всех анализируемых величин денежное выражение, высчитать все с точностью до копейки, но большого смысла в этом нет. Практичнее пользоваться условными единицами. В простейшем и вполне допустимом случае можно пользоваться трехбалльной шкалой. Далее мы продемонстрируем, как это делается. При идентификации активов, то есть тех ресурсов и ценностей, которые организация пытается защитить, следует, конечно, учитывать не только компоненты информационной системы, но и поддерживающую инфраструктуру, персонал, а также нематериальные ценности, такие как репутация организации. Отправной точкой здесь является представление о миссии организации, то есть об основных направлениях деятельности, которые желательно (или необходимо) сохранить в любом случае. Выражаясь объектно-ориентированным языком, следует в первую очередь описать внешний интерфейс организации, рассматриваемой как абстрактный объект. Одним из главных результатов процесса идентификации активов является получение детальной информационной структуры организации и способов ее (структуры) использования. Эти сведения целесообразно нанести на карту ИС в качестве граней соответствующих объектов. Информационной основой сколько-нибудь крупной организации является сеть, поэтому в число аппаратных активов следует включить компьютеры (серверы, рабочие станции, ПК), периферийные устройства, внешние интерфейсы, кабельное хозяйство, активное сетевое оборудование (мосты, маршрутизаторы и т.п.). К программным активам, вероятно, будут отнесены операционные системы (сетевая, серверные и клиентские), прикладное программное обеспечение,

инструментальные средства, средства управления сетью и отдельными системами. Важно зафиксировать, где (в каких узлах сети) хранится программное обеспечение, и из каких узлов оно используется. Третьим видом информационных активов являются данные, которые хранятся, обрабатываются и передаются по сети⁴.

Следует классифицировать данные по типам и степени конфиденциальности, выявить места их хранения и обработки, способы доступа к ним. Все это важно для оценки последствий нарушений информационной безопасности. Управление рисками - процесс далеко не линейный. Практически все его этапы связаны между собой, и по завершении почти любого из них может возникнуть необходимость возврата к предыдущему. Так, при идентификации активов может оказаться, что выбранные границы анализа следует расширить, а степень детализации - увеличить. Особенно труден первичный анализ, когда многократные возвраты к началу неизбежны.

Этапы, предшествующие анализу угроз, можно считать подготовительными, поскольку, строго говоря, они напрямую с рисками не связаны. Риск появляется там, где есть угрозы. Краткий перечень наиболее распространенных угроз был рассмотрен нами ранее. К сожалению, на практике угроз гораздо больше, причем далеко не все из них носят компьютерный характер. Так, вполне реальной угрозой является наличие мышей и тараканов в занимаемых организацией помещениях. Первые могут повредить кабели, вторые вызвать короткое замыкание. Как правило, наличие той или иной угрозы является следствием пробелов в защите информационной системы, которые, в свою очередь, объясняются отсутствием некоторых сервисов безопасности или недостатками в реализующих их защитных механизмах. Опасность прогрызания кабелей возникает не просто там, где есть мыши, она связана с отсутствием или недостаточной прочностью защитной

⁴ Лопатин, В.Н. Информационная безопасность России: Человек, общество, государство. Серия: Безопасность человека и общества. М.: 2000. - 428 с.

оболочки. Первый шаг в анализе угроз - их идентификация. Рассматриваемые виды угроз следует выбирать исходя из соображений здравого смысла (исключив, например, землетрясения, однако, не забывая о возможности захвата организации террористами), но в пределах выбранных видов провести максимально подробный анализ. Целесообразно выявлять не только сами угрозы, но и источники их возникновения - это поможет в выборе дополнительных средств защиты. Например, нелегальный вход в систему может стать следствием воспроизведения начального диалога, подбора пароля или подключения к сети неавторизованного оборудования. Очевидно, для противодействия каждому из перечисленных способов нелегального входа нужны свои механизмы безопасности. После идентификации угрозы необходимо оценить вероятность ее осуществления.

Допустимо использовать при этом трехбалльную шкалу (низкая (1), средняя (2) и высокая (3) вероятность). Кроме вероятности осуществления, важен размер потенциального ущерба. Например, пожары бывают нечасто, но ущерб от каждого из них, как правило, велик. Тяжесть ущерба также можно оценить по трехбалльной шкале. Оценивая размер ущерба, необходимо иметь в виду не только непосредственные расходы на замену оборудования или восстановление информации, но и более отдаленные, такие как подрыв репутации, ослабление позиций на рынке и т.п. Пусть, например, в результате дефектов в управлении доступом к бухгалтерской информации сотрудники получили возможность корректировать данные о собственной заработной плате. Следствием такого состояния дел может стать не только перерасход бюджетных или корпоративных средств, но и полное разложение коллектива, грозящее развалом организации. Уязвимые места обладают свойством притягивать к себе не только злоумышленников, но и сравнительно честных людей. Не всякий устоит перед искушением немного увеличить свою зарплату, если есть уверенность, что это сойдет с рук. Поэтому, оценивая вероятность осуществления угроз, целесообразно исходить не только из среднестатистических данных, но учитывать также специфику конкретных

информационных систем. Если в подвале дома, занимаемого организацией, располагается сауна, а сам дом имеет деревянные перекрытия, то вероятность пожара, к сожалению, оказывается существенно выше средней. После того, как накоплены исходные данные и оценена степень неопределенности, можно переходить к обработке информации, то есть собственно к оценке рисков. Вполне допустимо применить такой простой метод, как умножение вероятности осуществления угрозы на предполагаемый ущерб. Если для вероятности и ущерба использовать трехбалльную шкалу, то возможных произведений будет шесть: 1, 2, 3, 4, 6 и 9. Первые два результата можно отнести к низкому риску, третий и четвертый - к среднему, два последних - к высокому, после чего появляется возможность снова привести их к трехбалльной шкале. По этой шкале и следует оценивать приемлемость рисков⁵.

Правда, граничные случаи, когда вычисленная величина совпала с приемлемой, целесообразно рассматривать более тщательно из-за приближенного характера результата. Если какие-либо риски оказались недопустимо высокими, необходимо их нейтрализовать, реализовав дополнительные меры защиты. Как правило, для ликвидации или нейтрализации уязвимого места, сделавшего угрозу реальной, существует несколько механизмов безопасности, различных по эффективности и стоимости. Например, если велика вероятность нелегального входа в систему, можно потребовать, чтобы пользователи выбирали длинные пароли (скажем, не менее восьми символов), задействовать программу генерации паролей или закупить интегрированную систему аутентификации на основе интеллектуальных карт. Оценивая стоимость мер защиты, приходится, разумеется, учитывать не только прямые расходы на закупку оборудования и/или программ, но и расходы на внедрение новинки и, в частности, обучение и переподготовку персонала.

⁵ Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008. – 57 с.

Заключение

С усложнением информационных технологий предприятия

сталкиваются все с более сложными информационными рисками. Если бы была возможность обнаружить и определить уязвимость безопасности в процессе создания продукта деятельности то оправданы ли будут затраты на разработку таких методов?

Многие предприятия тонут в потоке данных. В большинстве случаев имеющееся количество фактов позволяет получать необходимую информацию по оцениванию информационной безопасности. Но проблема в том что не всегда и не все могут получать эту информацию. Решением этой задачи является механизм который позволит анализировать факты и выделяя необходимую информацию оценивать ее преобразуя в знания о безопасности.

Список литературы

1. Галатенко, В.А. Основы информационной безопасности. Интернет-

университет информационных технологий . ИНТУИТ.ру, 2008.

2. Галатенко, В.А. Стандарты информационной безопасности.

Интернет-университет информационных технологий. ИНТУИТ.ру, 2005.

3. Лопатин, В.Н. Информационная безопасность России: Человек, общество, государство. Серия: Безопасность человека и общества. М.: 2000.

4. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008.

5. Щербаков, А.Ю. Современная компьютерная безопасность.

Теоретические основы. Практические аспекты. М.: Книжный мир, 2009.