УДК 004
JEL коды: D89
08.00.13

Аудит компьютерной (информационной) системы в экономике, бизнесе
Audit of computer (information) system in economy, business

Омельченко И.В.
д.э.н., Тамбовский государственный университет имени Г.Р. Державина, Россия.
Omelchenko I.V.
Doctor of Economics, Tambov State University named after G.R. Derzhavina, Russia.

Аннотация
В работе рассмотрена актуальная для экономических, бизнес-систем задача системного анализа, формализации подсистем безопасности, проведения аудита информационной системы, минимизации рисков и ущерба. Методами системного анализа, теоретико-графовыми проведен анализ целей, проблем, методики, решений внутреннего и внешнего аудита корпорации. Предложены оценочные критерии, алгебраические подход к моделированию системы.
Abstract
The paper considers the task of system analysis, formalization of security subsystems, audit of information system, minimization of risks and damage, actual for economic, business systems. Methods of system analysis, graph-theoretic analysis of the goals, problems, methods, decisions of internal and external audit of the corporation. Estimation criteria, algebraic approach to system modeling are offered.
Ключевые слова: аудит, компьютерная, информационная, система, модель, граф, отношение, экономика, бизнес, стандарт безопасности.
Keywords: audit, computer, information, system, model, graph, attitude, economics, business, safety standard.

Постановка задачи

Информационная защищенность бизнес-систем – реальная необходимость. Организации, компании, осознавая ее, внедряют (как минимум, изучают, исследуют) релевантную политику безопасности, охватывающую не только компьютерные среды, но и информационный менеджмент [1, С. 62], [2, С. 109].

У каждой – свои требования по степени защиты и угрозам: волнуют DDoS-атаки, взлом, инсайд и др. Но все бизнес-компании стремятся минимизировать риски, ущерб [3, С. 14]. Независимый аудит позволит выявить уязвимости, оценить безопасность, ее уровень.

Аудит информационной системы (ИС) – сбор информации для установления, насколько:

обеспечиваются безопасность ИС, параметры целостности ресурсов;

достигаются цели системы.

Известны схемы (стандарты) аудита, например, BS 7799 (Великобритания), AICPA (США).

Согласно BS7799 [4, С. 29], [5, С. 17] для успешности сертификации проверяются:

1. инфраструктура (подсистема, сотрудники безопасности);
2. политика инфобезопасности (риск-менеджмент, обоснования защиты, механизма рисков, контроля безопасности, е-журналы фиксации проверок,

документы по администрированию, оцениванию, реализации требований стандарта, контрмерам по противодействию рискам [6] или маркерный контроль [7, С. 19]).

Для реализации в ИС релевантной аудит-системы необходима формализация не только положений, целей аудита, но и методики прогноза, необходимы прогнозирование, моделирование, системный подход. Этому посвящена работа.

Подготовка к процедурам аудита, сертификации

Документация, предоставляемая аудиторам, включает описания уровней защиты ИС (границы), риск-оценок, риск-управления [8, С. 362], инструментариев, обеспечивающих безопасность, ведомость соответствия. Здесь возможны и случайные ошибки.

Внутренний аудит, соответствие безопасности требованиям стандарта, включает проверку [9, С. 209] реализуемости норм стандарта. Например, возможные ответы аудитора:

1. уровень выполнения требований максимален, сопровождается достаточными компетенциями, контрольными мероприятиями, эффективными в достаточной мере;
2. уровень – высокий (компетенции, контроль – высокие);
3. уровень – хороший (компетенции, контроль – на необходимом уровне);
4. уровень – допустимый (компетенции, контроль, за исключением второстепенных требований, – на необходимом уровне);
5. уровень, недостаточный для решения, ответа (компетенции, контроль основных требований – недостаточны, не сформированы);
6. уровень полного несоответствия (компетенции, контроль не соответствуют требованиям, либо они к системе неприменимы).

Эта не единственная, полная система классификационных оценок. Шкалирование оценок аудитора позволяет описывать соответствия факторам амплитуд и весов (аналогично [10, С. 163]). Амплитуда – степень соответствия требованиям (позволяет разграничить реальные данные и субъективные оценки важности).

Для требования, не выполняемого совсем (или частично), указывается причина, ее категория:

1. не учитываемые раньше (причины, считавшиеся несущественными);
2. с финансовыми (ресурсными) ограничениями;
3. препятствующие факторам внешнего воздействия;
4. препятствующие фактором социокультурным;
5. с временными ограничениями;
6. без подходящих приложений и др.

Экспертами заполняется «Ведомость соответствия», аргументируется возможные (наблюдаемые) допустимые отклонения от стандарта.

Аудитор собирает доказательства, что ИС отвечает нормам стандарта, проанализировав документы, экспертные заключения.

Проверяется наличие (релевантность):

1. инфраструктуры безопасности, корректное распределение обязанностей персонала службы инфобезопасности, риск-менеджмента [11, С. 173];

2. политики инфобезопасности организации, методики, организационные меры и др.;
3. процедур идентификации меры безопасности (электронные журналы, администрирование и др.).

Аудит согласно стандарту BS7799

Аудитор готов провести анализ ключевых моментов безопасности, учитывая особенности, специфику бизнеса, ценность защищаемого ресурса, уровни возможных рисков. Формируется список отклонений от требований стандарта, эти несоответствия категорируются на категории:

1. существенные (ключевые требования не выполнены, либо используются нерелевантные меры оценки качеств информации);
2. несущественные (требования второстепенные, приводящие к снижению эффективности защиты – не выполнены).

При значительном обнаруженном количестве несущественных несоответствий, аудитор делает заключение (по совокупности) о несоответствии существенном. Учитываются методы [12.с.113] оценивания рисков.

Планирование, проведение аудита

Любой аудит – плановый, подготавливается (план обязателен). Аудитор знакомится с планом, требованиями компании. Сертификация стартует с анализа документации (политика безопасности, механизм оценивания вероятных рисков). Завершив аудит, представляют отчет, отражающий цели безопасности достижимы (реалистичность), соответствия (не противоречивости стандарту), релевантность, адекватность [13, С. 184] описаны полно.

Аудиторским планом определяется соответствие стандарту, он прилагается к аудиторскому отчету. Заказчик предоставляет сведения по организационной структуре. Сертифицируемая организация, стремящаяся соответствовать BS7799 и обладающая системой качества согласно ISO 9001:9002, может совместить сертификацию также по этим стандартам.

Аудит-процессы стартуют с официального собрания, где менеджменту, ИТ-персоналу разъясняют цели, методы оценки, устранения, замечания, план, доступ к документации, возможные сложности, меры по их преодолению, работу с данными (аудит, возможно, потребует доступа к критически защищаемым звеньям ИС).

Заключительное, постаудиторское собрание рассматривает результаты аудита, замечания, предложения, выводы. Участников официально регистрируют. Для безопасности все хотят приобретать лишь реально необходимое для надежной безопасности, минимизируя расходы, ущербы.

Риски, ущерб – категории, классы

Возможны ущербы:

1. репутационные;
2. социальной инженерии [14, С. 1];
3. от разглашения, инсайдерства;
4. восстановления (затраты на восстановление) ресурсов;

5. от невыполненных (третьей стороне) обязательств;
6. дезорганизации деятельности персонала, структур;
7. от нарушения договоров, партнерских отношений.

Часто ущерб – случайного характера. В праве, ущербом считается имущественные последствия правонарушений, ведущие к невыгодам (сокращение наличия имущества, недополученная прибыль, репутационный ущерб).

Классы угроз ИС:

1. конфиденциальности (хищение, несанкционированное копирование, обработка);
2. утечка самой информации или средств (носители, обработка);
3. блокирование информации, средств, их уничтожение;
4. целостности – модифицирование информации или ее искажение;
5. предъявление ложной, отрицание истинной информации.

Классы источников – субъект, объект, процесс (внутрисистемный, инсайдерский), внешние источники (техногенные, антропогенные, криминальные, недобросовестные, чрезвычайные – стихийные, ЧС).

Графовая формальная модель анализа рисков в ИС

Защита ИС – комплексная система, включающая различные средства, меры, инструментарий, методики. Необходимо оценить систему информационной защиты, степень необходимого взаимодействия ее подсистем, элементов. Следует выдвинуть релевантные гипотезы, формализовать, построить и исследовать адекватную модель защиты, реализовать эффективный алгоритм оценки защищенности. Иначе невозможны постановка задачи прогноза инфобезопасности, анализ, поиск уязвимостей [15, С. 35].

Результат анализа – количественная оценка инфобезопасности ИС, например, функционалом времени гарантированной защищенности, эволюции безопасности [16, С. 102].

Теории графов, логики позволяют строить математическую модель степени защищенности ИС. Математическое моделирование безопасности – основа решения задач, возникающих на уровне проекта, разработки, обслуживания. Формальное представление – возможность точного выбора мер безопасности ИС, архитектуры, реализации защиты [17, С. 51].

Предлагаемые сейчас модели анализа, аудита рисков не без недостатков [18, С. 159]. Предложим следующий подход. Пусть объект $o \in O$ – ресурс, используемый ИС. Множество O объектов – конечное. Каждому объекту присваиваем ранг (ранг безопасности) $r \in R$ представляющий собой аналог понятия метки в ОС.

Пусть R – множество (конечное) рангов системы. На R строим бинарное отношение " $\leq$ ":

1) $\forall\, r_1 \in R$ выполнено $r_1 \leq r_1$ (рефлективность);

2) $\forall\, r_1, r_2, r_3 \in R, r_1 \leq r_2$ и $r_1 \leq r_3$ выполняется $r_1 \leq r_3$ (транзитивность);

3) $\forall\, r_1, r_2 \in R$, $r_1 \leq r_2$ и , $r_2 \leq r_1$ выполняется , $r_2 = r_1$ (антисимметричность).

Отношение линейное, если $\forall\, r_1, r_2 \in R$ либо $r_1 \leq r_2$, либо $r_2 \leq r_1$. Отношение – отношение порядка, частичного (линейного) [19,с.163]. Определяем операции минимизации, максимизации рангов:

$$(a = \max_{r \in R}(r)) \Leftrightarrow (\{a \in R \mid \forall\, r \in R \longrightarrow r \leq a\}),$$

$$\left(a = \min_{r \in R}(r)\right) \Leftrightarrow (\{a \in R \mid \forall\, r \in R \longrightarrow r \leq a\}\Big).$$

Субъект s – организация, группа, пользователь, администратор, программа, техническое (технологическое) средство, базовое для функционирования ИС. Тогда S – множество (конечное) субъектов, взаимодействующих с ИС. В него введем дополнительный субъект – злоумышленник, воздействующий извне системы.

На множестве пар $S \times O$ зададим отображение $g: S \times O \longrightarrow R$, ставящее паре вида (субъект, объект) вполне определенный ранг. Для субъекта s без доступа к объекту o

$$g(s, o) = \min_{r \in R}(r)).$$

Ранг субъекта s определяется выражением:

$$rang(s) = \max_{r \in R}\big(g(s, o)\big).$$

Злоумышленнику соответствует минимальный ранг субъектов (обозначим 0):

$$rang(s) = \min_{r \in R}(r) = 0.$$

Построим взвешенный орграф $G(S, U, f, p)$, множество вершин – S. С каждой вершиной ассоциирован ее ранг. Веса дуг $u \in U, p(u) \in [0; 1]$ определяют вероятности несанкционированного доступа субъекта s субъектом t ((s, t) – дуга u).

Исходя из практической возможности маловероятные события доступа (близости нулю) – не рассматриваются. Выбирается пороговая вероятность и из графа удаляются дуги веса меньше δ:

$$U' = \{u \in U \mid p(u) \geq \delta\}$$

Возможны различные стратегии поведения злоумышленника, в зависимости характера угроз. Например, ресурсами являются компьютеры пользователей и корпоративный сервер БД (доступ к документам пользователя, хранимым на сервере данным), а субъекты – пользователи компьютеры. В качестве множества рангов выберем числовой отрезок.

С каждым правилом безопасности можно ассоциировать вес, зависящий от ранга правила, количества участников применяющих его, степени взаимодействия. Стоимость пути определяется стоимостями всех примененных правил. Используя их, можно воспроизводить состояние при изменениях доступа, получая возможности анализа возможных угроз, например, без содействия владеющего такими правами.

Анализ защищенности от злоумышленника извне ИС

Предположим, злоумышленник передвигается по ориентированной простой цепочке к вершине ранга r. Известны веса дуг, исходящих из текущей вершины. Очевидно, злоумышленник выберет дугу максимального веса (высокая вероятность взлома), будет двигаться, пока не вершина ранга r не будет достигнута (либо это окажется невозможным).

Если он попадет в вершину, дальнейшее движение из которой невозможно, злоумышленник возвращается обратно на шаг, выбирает новую дугу (следующую за выбранной, веса убывающие). Обозначим построенную ориентированную цепь через $z\,(s, r)$. Пусть $|z(s, r)|$ – произведение весов всех дуг цепи. Вероятность доступа злоумышленника к объекту ранга r оценим:

$$p(r) = \max_{s \in S | rang(s) = 0|} (|z(s, r)|)\,.$$

Анализ внешней защищенности ИС

Обозначим $z\,(s,t)$ – ориентированную цепь наибольшей вероятности произведения весов дуг *(s,t)*. Поиском таких объектов занимается модифицированная задача о кратчайшем пути на графах [20,с.107]. Вероятность доступа извне к объекту ранга r :

$$P(r) = \max_{s\in S|rang(s)=f} \left(\max_{t\in S|rang(t)=t} |z(s,t)| \right).$$

Сложности формализации сложноорганизованной ИС

К сложностям, недостаткам рассмотренной модели (и других) следует отнести сложность формализации семантики безопасного состояния, поведения объектов. Проверка релевантности программ безопасности изначальным спецификациям, формализованным моделям опирается на статистический и графов анализ, формальную верификацию («model checking»), ситуационное (включая событийное) моделирование.

Эти методы, их реализации, инструментарий, имеют ограниченное практическое использование. Например, имитационное моделирование – из-за сложности математического описания эвристических процедур, графовые – из-за алгоритмической сложности, верификация – из-за сложности проведения, использования, тестирование – из-за валидности, мониторинга.

У многих – общие «проблемы»: «полноты покрытия» целевой программы, строгости доказательства, декомпозиции процесса и последующей композиции и др. В процессе апробации методов стратегии информационной безопасности ИС формируется формально-понятийный аппарат, методы, средства (включая нормативно-правовые). Важно развивать их, создавать инструментальные средства.

Для эффективной формализации, структурирования следует привлечь математиков, информатиков, психологов, специалистов по безопасности и др., способных прогнозировать критичность ситуации, оценить риски, построить, исследовать модели киберугроз, принять решение, улучшить политику безопасности.

Заключение

Степень защищенности в идеале от действий злоумышленника не зависит, как и от выбранной им стратегии. Это позволяет получать стационарные по времени характеристики защищенности, формировать политику безопасности. Графовую модель защищенной системы можно применять для получения стационарных характеристик защищенности. Попытка уже сделана. На сегодняшний день для изучения неравновероятных вариантов графа используется метод моментов [20].

Литература

1. Климов С.М. Методы и модели противодействия компьютерным атакам.-Люберцы: КАТАЛИТ, 2008.
2. Уродовских В.Н. Управление рисками предприятия: учеб. пособие для вузов. -М.: Вузовский учебник. ИНФРА-М, 2012.-168 с.
3. Graham J.H., Ralston P.S. Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements // International Journal of Information Management.-2008.-28(6).
4. British Standard. Code of practice for information security management / British Standards Institution, BS 7799:1995.
5. British Standard. Information security management systems - Specification with guidance for use British Standards Institution, BS 7799-2:2002.

6. Рейнольдс Дж., Холбрук П. Руководство по информационной безопасности предприятия**,** JetInfo, 1996, 10-11.
7. Щеглов К.А., Щеглов А.Ю. Принцип и метод маркерного контроля доступа к создаваемым объектам// Вопросы защиты информации. Научно-практический журнал. Выпуск 1 (96), Москва, 2012.
8. Батищев Р.В., Афанасьева А.С. Анализ и управление рисками применительно к автоматизированным системам с заданным количеством поражаемых объектов. // Информация и безопасность (регион. науч.-техн. журнал).-Воронеж,2007, вып.2, с.362.
9. Железняк В.П. Случайные величины ущерба в атакуемых компьютерных подсистемах // Информация и безопасность (регион. науч.-техн. журнал).-Воронеж, 2007, т.10, ч.4. -с.621.
10. Казиев В.М. Обобщенная шкала оценок учебных достижений студента / Труды Всероссийской научно-практической конференции «Информационные технологии в обеспечении нового качества обучения» (14 апреля 2010). -М.: НИТУ МИСиС, с.160-174.
11. Гончаренко Л.П., Филин С.А. Риск-менеджмент. -М.: КНОРУС, 2006.-216 с.
12. Петренко С.А. Метод оценивания информационных рисков организации // Проблемы управления информационной безопасностью. – М.: Едиториал УРСС, 2002.-с.112-124.
13. Исаев И.В. ИТ риски и информационная безопасность // Современные наукоемкие технологии.–2014.–№7-1, с.184-184. URL: http://www.top-technologies.ru/ru/article/view?id=34276 (дата обращения: 02.06.2018).
14. Попов А. Атаки на информацию с помощью методов социальной инженерии // JetInfo, №3, 2015. URL: http://www.jetinfo.ru/jetinfo_arhiv/konsalting-v-ib-kaznit-nelzya-pomilovat/chelovek-cheloveku/2015 (доступ 02.05.2018).
15. Забродский В., Капустин Н. Теоретические основы оценки экономической безопасности отрасли и фирмы // Бизнес-информ, 2013, №15–16, с.35–37.
16. Гладких Е.Л. Эволюция экономической безопасности // Ростовский научный журнал, 2016, т.8,№11. с.100-116
17. Коллектив авторов. Теоретико-графовый подход к анализу рисков в вычислительных сетях / А.В. Аграновский, Р.А. Хади, В.Н. Фомченко, А.П. Мартынов, В.А. Снапков // Защита информации. Конфидент, №2, 2002, с.50-53.
18. Ансофф И. Стратегическое управление. -М.:Алмаз-пресс, 2013.–230с.
19. Гуров С.И. Булевы алгебры, упорядоченные множества, решетки: определения, свойства, примеры (2-ое изд.).-М.: Либроком, 2013.-352с.
20. Оре О. Теория графов. –М.: УРСС, 2008. -352с.

References

1. Klimov S.M. Methods and models of counteraction to computer attacks. -Lyubertsy: CATALIT, 2008.
2. Urodovskikh V.N. Enterprise Risk Management: Textbook. manual for universities. -M .: University textbook. INFRA-M, 2012.-168 p.
3. Graham J.H., Ralston P.S. Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements // International Journal of Information Management.-2008.-28 (6).
4. British Standard. Code of practice for information security management / British Standards Institution, BS 7799: 1995.
5. British Standard. Information security management systems - Specification with guidance for the use of the British Standards Institution, BS 7799-2: 2002.
6. Reynolds J., Holbrook P. Information Security Guide for the Enterprise, JetInfo, 1996, 10-11.
7. Shcheglov K.A., Scheglov A.Yu. Principle and method of marker access control to objects being created // Issues of information protection. Scientific and practical journal. Issue 1 (96), Moscow, 2012.
8. Batishchev R.V., Afanasyeva A.S. Analysis and risk management in relation to automated systems with a specified number of affected objects. // Information and Security (Region: Scientific and Technical Journal) .- Voronezh, 2007, issue 2, p.362.
9. Zheleznyak V.P. Random amounts of damage in the attacked computer subsystems // Information and Security (Region Scientific and Technical Journal) .- Voronezh, 2007, vol. 10, p.4. -p.621.
10. Kaziev V.M. Generalized scale of assessments of student's academic achievements / Proceedings of the All-Russian Scientific and Practical Conference "Information Technologies in Ensuring a New Quality of Learning" (April 14, 2010). -M .: NITU MISiS, p.160-174.
11. Goncharenko LP, Filin S.A. Risk management. -M .: Knorus, 2006.-216 p.
12. Petrenko S.A. Method of assessing the organization's information risks // Problems of information security management. - M .: Editorial URSS, 2002.-p.112-124.
13. Isaev I.V. IT risks and information security // Modern science-intensive technologies.-2014.-№7-1, p.184-184. URL: http://www.top-technologies.ru/en/article/view?id=34276 (reference date: 02/06/2018).
14. Popov A. Attacks on information using social engineering techniques. // JetInfo, №3, 2015. URL: http://www.jetinfo.ru/jetinfo_arhiv/konsalting-v-ib-kaznit-nelzya-pomilovat/chelovek- cheloveku / 2015 (accessed on 05/02/2018).

15. Zabrodsky V., Kapustin N. Theoretical bases of an estimation of economic safety of branch and firm // Business-inform, 2013, №15-16, p.35-37.

16. Gladkikh E.L. The evolution of economic security / Rostov scientific journal, 2016, vol. 8, No. 11. p.100-116

17. The team of authors. The graph-graph approach to risk analysis in computer networks / A.V. Agranovsky, R.A. Hadi, V.N. Fomchenko, A.P. Martynov, V.A. Snapkov // Protection of information. Confident, №2, 2002, pp. 50-53.

18. Ansoff, I. Strategic Management. -M.: Diamond press, 2013.-230s.

19. Gurov SI Boolean algebras, ordered sets, lattices: definitions, properties, examples (2nd ed.) .- M .: Librocom, 2013.-352p.

20. Ore O. Theory of graphs. -M .: URSS, 2008. -352c.