УДК: 657.6.004.056.226(5)

РИСК - ОРИЕНТИРОВАННЫЙ ПОДХОД К ПРОВЕДЕНИЮ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аскарова М.М., Эркинбаев Т. Д., Абдиева Л.К., Осмонканов А.М.
КГТУ им.И.Раззакова

В статье рассматривается значимость аудита безопасности в современных организациях и его влияние на эффективное управление рисками и защиту информации. Рассматривается аудит как инструмент анализа внешних и внутренних угроз безопасности, выявления регуляторных и юридических рисков, предотвращения мошенничества и защиты коммерческой тайны. Особое внимание уделяется риск-ориентированному подходу, анализу бизнес-процессов и разработке рекомендаций по улучшению безопасности.

Ключевые слова: Аудит безопасности, угрозы безопасности, риски, информационная защита, риск-ориентированный подход, бизнес-процессы, рекомендации, мошенничество, коммерческая тайна, устойчивость организации.

ТОБОКЕЛЧИЛИК- АУДИТТИН МААЛЫМАТТЫК КООПСУЗДУГУН ӨТКӨРҮҮГӨ КАРАТА БАГЫТТАЛГАН МАМИЛЕ

Аскарова М.М., Эркинбаев Т. Д., Абдиева Л.К., Осмонканов А.М.
И.Раззакова атн. КМТУ

Макалада заманбап уюмдардагы коопсуздук аудитинин мааниси жана анын тобокелдиктерди натыйжалуу башкарууга жана маалымат коопсуздугуна тийгизген таасири каралат. Аудитти коопсуздуктун тышкы жана ички коркунучтарын талдоо, ченемдик-укуктук тобокелдиктерди аныктоо, алдамчылыктын алдын алуу жана коммерциялык сырды коргоо куралы катары каралат. Тобокелге негизделген мамилеге, бизнес процесстерин талдоого жана коопсуздукту жакшыртуу боюнча сунуштарды иштеп чыгууга өзгөчө көңүл бурулат.

Баштапкы сөздөр: Коопсуздук аудити, коопсуздук коркунучтары, тобокелдиктер, маалыматты коргоо, тобокелге негизделген мамиле,

бизнес процесстери, сунуштар, алдамчылык, коммерциялык сырлар, уюмдун туруктуулугу.

RISK - A RISK-ORIENTED APPROACH TO INFORMATION SECURITY AUDIT

Askarova M.M., Erkinbaev T. D., Abdieva L. K., Osmonkanov A.M.
KSTU named of I.Razzakov

The article discusses the importance of security auditing in modern organizations and its impact on effective risk management and information protection. The audit is considered as a tool for analyzing external and internal security threats, identifying regulatory and legal risks, preventing fraud and protecting trade secrets. Particular attention is paid to a risk-based approach, business process analysis and development of recommendations for improving security.

Keywords: Security audit, security threats, risks, information protection, risk-based approach, business processes, recommendations, fraud, trade secrets, organization sustainability.

Сегодня многие компании широко применяют риск-ориентированный подход, который основывается на оценке рисков согласно принятой в индустрии методологии и передовым практикам. Этот подход позволяет принимать решения о реализации мер по улучшению системы информационной безопасности и защите на основе выявленных рисков. Эффективно построенный процесс риск-менеджмента дает руководителям информационной безопасности возможность самостоятельно определить необходимые меры для снижения неприемлемых рисков. Он также помогает сэкономить бюджет, избегая нецелесообразных затрат на защиту неподходящих систем, процессов или направлений бизнеса, и обосновать выделение дополнительных ресурсов на защиту новых областей деятельности компании, с учетом требований compliance.

На сегодняшний день у многих иностранных компаний, специализирующихся в области решения комплексных проблем информационной безопасности (ИБ), существуют собственные методики

управления информационными рисками. Эти методики отличаются по уровню и совершенству используемых математических методов, которые лежат в основе процедур оценки рисков. В зависимости от этого они обладают различными возможностями для адекватного учета реальных факторов, что, в свою очередь, определяет точность и надежность полученных оценок риска.

Важно выбрать подходящий метод и средство анализа рисков информационной безопасности, учитывая особенности организации и ее потребности. В таблице 1 каждый из этих методов имеет свои достоинства и недостатки:

Таблица 1. Методология анализа рисков информационной безопасности, их достоинства и недостатки

Методология	**Достоинства**	**Недостатки**
Метод CORAS	- Компьютеризированный инструмент для моделирования риска	- Отсутствие периодичности оценки рисков и обновления их величин
	- Возможность документирования и создания отчетов о результатах анализа	- Неоценка эффективности инвестиций в безопасность
		- Невозможность нахождения баланса между мерами по предотвращению, выявлению, исправлению и восстановлению
		- Распространяется бесплатно, но требует значительных ресурсов для установки и применения
Метод OCTAVE	- Уделяет особое внимание угрозам и уязвимостям информационной безопасности	- Требует высокой степени экспертизы и опыта в области информационной безопасности

	- Способствует разработке конкретных и применимых мер безопасности	- Может быть сложным для организаций без соответствующей подготовки и опыта
		- Требует существенного времени и усилий для проведения анализа и разработки мер безопасности
Метод OWASP Risk Rating Method	- Специализированный метод для оценки рисков информационной безопасности веб-приложений	- Ограничен применением только в контексте веб-приложений
	- Имеет конкретные критерии и метрики для оценки рисков	- Ограничен применением только в определенной сфере (веб-приложения)
	- Разработан Open Web Application Security Project (OWASP)	- Не учитывает широкий спектр угроз и уязвимостей вне контекста веб-приложений

Каждый метод и средство анализа рисков информационной безопасности свои особенности и подходы. При выборе конкретного метода необходимо учитывать цели организации, доступные ресурсы, уровень экспертизы и предпочтения.

Важно отметить, что ни один метод не является универсальным и идеальным для всех ситуаций. Каждый метод имеет свои преимущества и ограничения, и их выбор зависит от специфики организации и требований к анализу рисков информационной безопасности.

При использовании любого метода анализа рисков информационной безопасности важно учитывать контекст организации, ее уязвимости, ценности и уровень риска, а также принимать во внимание регуляторные и законодательные требования.

В конечном итоге, правильный выбор метода и средств анализа рисков информационной безопасности позволит организации более

точно оценить угрозы, принять обоснованные решения и разработать эффективные меры для обеспечения безопасности информации.

Анализ уязвимостей веб-приложений с использованием метода OWASP

Метод OWASP Risk Rating Method (метод оценки риска OWASP) является одним из подходов для оценки уязвимостей веб-приложений, разработанным OWASP (Open Web Application Security Project) - сообществом экспертов по информационной безопасности. Данный метод основан на систематическом анализе и оценке различных аспектов уязвимостей, позволяя определить их уровень риска для веб-приложений.

Угрозы, связанные с аутентификацией:

- Слабые пароли: пользователи могут выбирать простые пароли или использовать один и тот же пароль для разных сервисов.

Уязвимости веб-приложений:

- **Межсайтовый скриптинг (XSS):** возможность внедрения вредоносных скриптов в веб-страницы, которые выполняются на стороне клиента. Пример скрипта на JavaScript, который может помочь защитить от межсайтового скриптинга (XSS):

```
gh.js > ...
function sanitizeInput(input) {
  // Замена опасных символов на их HTML-сущности
  const sanitizedInput = input
    .replace(/&/g, '&amp;')
    .replace(/</g, '&lt;')
    .replace(/>/g, '&gt;')
    .replace(/"/g, '&quot;')
    .replace(/'/g, '&#x27;')
    .replace(/\//g, '&#x2F;');

  return sanitizedInput;
}

// Пример использования:
const userInput = "<script>alert('XSS!');</script>";
const sanitizedUserInput = sanitizeInput(userInput);
console.log(sanitizedUserInput);
```

Рис. 1. Скрипт представляющего функцию sanitizeInput

Этот скрипт представляет функцию sanitizeInput, которая заменяет опасные символы на соответствующие HTML-сущности. Это позволяет

корректно отобразить пользовательский ввод на веб-странице, не выполняя вредоносные скрипты.

В приведенном примере, если пользователь вводит <script>alert('XSS!');</script>, функция sanitizeInput заменяет символы <, >, &, ", ', / на соответствующие HTML-сущности.

Таким образом, пользовательский ввод будет отображаться как обычный текст на веб-странице, и скрипты не будут выполняться.

Важно отметить, что данная функция только обрабатывает пользовательский ввод для предотвращения XSS-атак. Чтобы обеспечить полную защиту от XSS, рекомендуется также использовать Content Security Policy (CSP), фильтрацию входных данных на сервере и другие соответствующие меры безопасности.

- **Межсайтовая подделка запроса (CSRF):** возможность выполнения нежелательных действий от имени авторизованного пользователя без его согласия. Пример PHP-кода, который поможет защитить от межсайтовой подделки запроса (CSRF):

Рис. 2. Использования сессии для хранения токена CSRF.

Функция generateToken генерирует случайный токен и сохраняет его в сессии. Функция validateToken проверяет, соответствует ли предоставленный пользователем токен сохраненному токену в сессии.

При генерации формы, скрытое поле csrf_token содержит значение токена CSRF, которое передается вместе с остальными данными при отправке формы. При обработке POST-запроса, код проверяет переданный пользователем токен на соответствие сохраненному токену в сессии. Если токены совпадают, запрос считается действительным и может быть обработан. В противном случае, запрос отклоняется как потенциально поддельный.

Это базовая реализация защиты от CSRF, но для обеспечения более надежной защиты, рекомендуется также использовать дополнительные меры, такие как добавление временного ограничения действия токена, проверка Referer-заголовка, использование двухфакторной аутентификации и другие меры безопасности.

Выводы: В заключении, метод OWASP Risk Rating предоставляет ценные инсайты о рисках, связанных с уязвимостями веб-приложений. Его использование помогает выявить приоритетные уязвимости и разработать рекомендации по их устранению. Этот метод является важным инструментом для эффективного управления уязвимостями и обеспечения безопасности веб-приложений.

ЛИТЕРАТУРА

1. Толчинская М.Н. Риск-ориентированный подход в организации службы внутреннего аудита // Фундаментальные исследования. – 2015. – № 10-3. – С. 640-644;
2. Шаханова М.В. Современные технологии информационной безопасности: Учебнометодический комплекс. ДВФУ, 2013. 180 с.

3. Калужин Е.А., Монастырский Д.С. Алгоритм выбора средств информационной безопасности при проектировании системы защиты информации // Modern Sciencs, 2016. № 11. С. 24-27.
4. Bjorn A.G. CORAS, A Platform for Risk Analysis on Security Critical Systems - Modelbased Risk Analysis Analysis Targeting Security, 2002.