

INTOSAI



## *Методика проверки безопасности информационных систем*

КОМИТЕТ ПРОФЕССИОНАЛЬНЫХ СТАНДАРТОВ (PSC) ИНТОСАИ

СЕКРЕТАРИАТ КОМИТЕТА ПРОФЕССИОНАЛЬНЫХ СТАНДАРТОВ

RIGSREVISIONEN • STORE KONGENSGADE 45 • P.O. Box 9009 • 1022 COPENHAGEN K • DENMARK

Тел.: +45 3392 8400 • Факс: +45 331 1 0415 • E-MAIL: [INFO@RIGSREVISIONEN.DK](mailto:INFO@RIGSREVISIONEN.DK)

ИНТОСАИ



Генеральный секретариат ИНТОСАИ – RECHNUNGSHOF  
(Счетная палата Австрийской Республики)  
DAMPFSCHIFFSTRASSE 2  
A-1033 VIENNA  
AUSTRIA

Тел.: ++43 (1) 711 71 • Факс: ++43 (1) 718 09 69

E-MAIL: [intosai@rechnungshof.gv.at](mailto:intosai@rechnungshof.gv.at);  
WORLD WIDE WEB: <http://www.intosai.org>

# **Методика проверки обеспечения безопасности информационных систем**

Руководство по проверке обеспечения безопасности информационных систем в государственных организациях

**Издан**

**Аудиторским комитетом электронной обработки данных**

**Международной организацией высших органов аудита**

**Октябрь 1995 г.**

## Содержание

Том 1	6
Обзор	7
Что такое безопасность информационных систем?	7
Инфраструктура защиты информации	9
Двухуровневый подход к проверкам обеспечения безопасности информационных систем	10
Нисходящий принцип проверки обеспечения безопасности информации - Том 2	12
Метод детализации обеспечения безопасности информационных систем - Том 3	14
Как применяется двухуровневый подход к проверкам информационных систем	15
Когда и как применяется метод нисходящей пошаговой детализации в проверке - Том 2	16
Когда и как применяются методы детализации в проверке обеспечения безопасности информации - Том 3	17
Том 2: Метод нисходящей пошаговой детализации	20
Введение	21
Процесс оценки компьютерной безопасности	22
Эволюция управления информацией	22
Управление безопасностью	23
Служба безопасности	23
Процесс	23
Заполнение формы "сообщение об уязвимости информации и определение категории защиты"	25
Заполнение формы "оценка последствий и угроз для деятельности"	26
Оценка угроз и рисков	26

Оценка последствий для деятельности	27
Оценка уровня риска нарушения безопасности	28
Сводная информация по оценкам обеспечения безопасности	30
Решение по обеспечению безопасности и рекомендуемые мероприятия	31
Шаги оценки компьютерной безопасности	32
ПРИЛОЖЕНИЕ А - Эволюция управления информацией	34
ПРИЛОЖЕНИЕ В - Процесс оценки обеспечения безопасности информационных систем	35
ПРИЛОЖЕНИЕ С - Сообщение об уязвимости информации и определение категории защиты	36
ПРИЛОЖЕНИЕ F - Таблица оценки уровня риска нарушения безопасности	40
ПРИЛОЖЕНИЕ Н - Исходные угрозы и меры безопасности	41
ПРИЛОЖЕНИЕ I – Определения	85
Том 3: Метод детализации обеспечения безопасности информационных систем	90
Обзор	91
Инфраструктура	92
Границы	94
Группа	94
Угрозы / уязвимость	96
Оценка	97
Требования к безопасности	99
Контрмеры	100
Управление безопасностью	101

# **Методика проверки обеспечения безопасности информационных систем**

## **Руководство по проверке обеспечения безопасности информационных систем в государственных организациях**

**Том 1:**

**Обзор**

## **Обзор**

Перед тем, как перейти к изучению других томов Руководства ИНТОСАИ по методике проверки обеспечения безопасности информационных систем (ISS), ознакомьтесь с содержанием настоящей главы. Здесь приводится описание структуры методики и условия ее использования.

Руководство по методике проверки обеспечения ISS применяется к любой среде (мейнфрейма, микрокомпьютера или локальной сети микрокомпьютеров).

Оно предлагает использовать двухуровневый подход. На 1-ом уровне высшим органам аудита (BOA) предлагается метод для выполнения простой не автоматизированной проверки информационных систем, особенно в случае ограниченных ресурсов или если в требованиях к составлению отчетности не указано иного (Том 2). 2-ой уровень представляет более сложный метод, который основывается на денежном выражении рисков нарушения безопасности информации (Том 3).

Главная задача настоящего руководства - помочь высшим органам аудита, которые обладают необходимыми полномочиями, в проверке программ обеспечения безопасности информационных систем, используемых различными государственными организациями. Высшие органы аудита также могут использовать руководство для настройки комплексных и экономически эффективных программ обеспечения безопасности, охватывающих ключевые информационные системы в собственном офисе. Настоящее руководство не является подробным руководством по аудиту безопасности. Оно лишь описывает структурированный подход к оценке и управлению рисками в информационных системах.

### **Что такое безопасность информационных систем?**

Программа обеспечения безопасности информационных систем предназначена для защиты информации организации путем снижения риска

потери конфиденциальности, целостности и доступности этой информации до приемлемого уровня.

Хорошая программа обеспечения безопасности информации включает два основных элемента: анализ рисков и управление рисками.

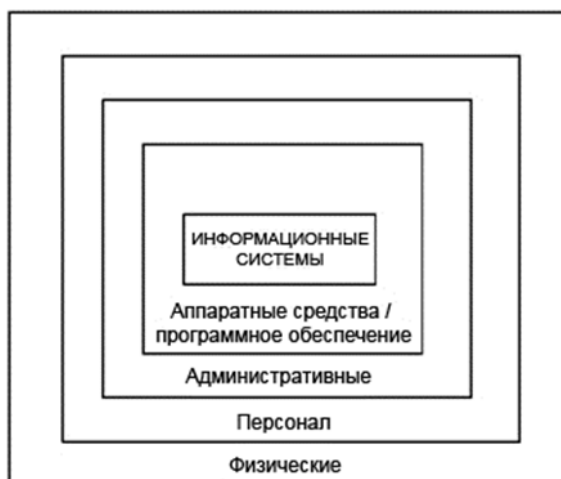
На этапе анализа рисков во внимание принимается реестр всех информационных систем. Определяется ценность каждой системы для организации и степень риска, которому подвергается организация. С другой стороны, управление рисками включает выбор средств контроля и мер безопасности, которые снижают подверженность организации риску до приемлемого уровня. Чтобы меры снижения риска были эффективными, результативными и отражали здравый смысл, они должны приниматься в пределах инфраструктуры безопасности, в которых меры общей безопасности дополняются мерами компьютерной, административной, кадровой и физической безопасности (см. таблицу 1).

Управление рисками становится проблемой высшего руководства. При управлении рисками необходимо достичь баланса между важностью информации для организации, с одной стороны, и стоимостью кадровых, административных и технических мер обеспечения безопасности, с другой стороны. Затраты на применяемые меры обеспечения безопасности должны быть меньше, чем потенциальный ущерб в результате потери конфиденциальности, целостности и доступности информации.

Многие официальные методики анализа рисков, имеющиеся на рынке, требуют технической экспертизы в области информационных технологий и релевантных средств контроля, а также наличия точных сведений о проявлениях угроз, которые могут происходить вне пределов досягаемости многих аудиторских управлений, по крайней мере, изначально. Поэтому задача заключается в накоплении со временем необходимой экспертизы и ресурсов.



Таблица 1 Дополнительные уровни защиты информации



### **Инфраструктура защиты информации**

Защита информации является единственным элементом инфраструктуры защиты и, по существу, не должна рассматриваться изолированно. Должна быть система стратегий безопасности, охватывающая все аспекты физической безопасности, кадровой безопасности и информационной безопасности. Должны быть четко определены роли и обязанности пользователей, сотрудников службы безопасности и Руководящего комитета по информационным системам. Программа обеспечения безопасности информации должна включать все стороны уязвимости корпоративной информации, включая конфиденциальность, целостность и доступность. Должна быть установлена программа оповещения о состоянии защиты, которая напоминает персоналу о возможных рисках и состоянии уязвимости, а также об их обязанностях как хранителей корпоративной информации.

Согласно таблице 1 безопасность информации представляет собой комплекс мер, принимаемых на физическом, кадровом, административном, компьютерном уровнях и уровне информационных систем. Меры должны работать все вместе. Безопасность информации представляет собой эффективный административный контроль, причем отсутствие такого

контроля на любом уровне может угрожать обеспечению безопасности на других уровнях. Например, если недостаточно хорошо разработаны и внедрены стратегии кадровой безопасности, тогда обеспечение защиты информации становится крайне дорогим или почти невозможным. С другой стороны, минимальные меры на всех уровнях должны обеспечивать минимальную защиту информации при условии, что риск, связанный с нарушением безопасности, невысок и приемлем руководством. Бывают также ситуации, когда меры по обеспечению безопасности на одном уровне могут компенсировать недостаток обеспечения безопасности на другом уровне. Например, шифрование обеспечивает дополнительный уровень защиты конфиденциальности и целостности данных даже в случаях, когда меры физической, кадровой или административной безопасности могут оказаться недостаточными. Шифрование остается одной из последних мер защиты, помогающей предотвратить нарушение конфиденциальности или целостности данных.

При планировании обеспечения безопасности информации важность информации для руководства и объем этой информации относительно информации других типов должны быть сопоставлены с основными ограничениями по обеспечению безопасности для носителей. Во многих государственных департаментах в случае отсутствия исключительных требований к переносу совершенно секретной информации на защищенный должным образом ноутбук, необходимо просто создать и перенести эту информацию каким-либо иным способом. Для таких департаментов стоимость и ограничения подходящих средств контроля и мер обеспечения безопасности могут просто не приниматься в расчет при небольшом объеме информации, которая подлежит защите.

### **Двухуровневый подход к проверкам обеспечения безопасности информационных систем<sup>1</sup>**

---

<sup>1</sup> Данный двухуровневый подход является результатом совместной работы Национального контрольно-ревизионного управления Соединенного Королевства и Управления Генерального аудитора Канады.

В настоящем руководстве представлен двухуровневый подход к проверкам обеспечения безопасности информационных систем. Особо подчеркивается использование здравого смысла в сопоставлении стоимости системы обеспечения безопасности, встраиваемой в систему, и важности информации, используемой этой системой<sup>2</sup>.

В случае ограниченных ресурсов многих высших органов аудита последним предлагается сначала использовать не автоматизированное представление управления безопасностью информации «сверху-вниз». Переход к второму этапу, к детальному анализу, цель которого денежная оценка риска нарушения информации, осуществляется высшими органами аудита, только если руководству нужно точно оценить денежное выражение обеспечения его решений или если оцениваются конкретные технические воздействия. Оба метода включают элементы анализа рисков и управления рисками (см. таблицу 2).

**Таблица 2. Двухуровневый подход к анализу и управлению рисками обеспечения безопасности**



<sup>2</sup> Безопасность в значительной степени носит предупредительный характер, как, например, страхование автомобиля. Даже если большинство людей никогда и не попадали в серьезные автомобильные аварии, они, тем не менее, страхуют свой автомобиль. Они получают выгоды от страховки только в случае аварии. Обеспечение безопасности информации «является законной и необходимой статьей расходов в управлении информацией. Государственные департаменты должны учитывать как стоимость внедрения средств контроля, так и потенциальные издержки, которые они понесут в случае невыполнения такой процедуры. Расходы на обеспечение безопасности должны быть соизмеримы с потребностью и должны быть включены в стоимость жизненного цикла любой компьютерной системы». (Управление Генерального аудитора Канады, Ежегодный отчет, 1990 г., глава 9, Аудит обеспечения безопасности информации)

Данный двухуровневый подход обеспечивает высшие органы аудита возможностями при выборе методик и последовательный переход от наименее сложной методики к формализованной методике с большим количеством ресурсов.

## **Нисходящий принцип проверки обеспечения безопасности информации - Том 2**

Метод нисходящей пошаговой детализации прост, но в то же время характеризует детальностью. С его помощью высшие органы аудита могут сделать выводы относительно рисков нарушения безопасности информационных систем, рассматриваемых в ходе проверки. Метод использует нисходящий принцип обеспечения безопасности информации, поскольку в его основе лежит точка зрения высшего руководства при определении того, какая информация является ценной для организации, каковы риски и последствия нарушения безопасности и какие рекомендации должны быть выполнены. Такой подход позволяет аудиторам сфокусировать свое внимание на ключевых информационных системах, в частности на тех, которые имеют особое значение при обеспечении безопасности.

Метод нисходящей пошаговой детализации основывается на качественных оценках риска возможных угроз и степени их последствий. Внимание фокусируется на оценке важности информации или данных, передаваемых через информационные системы, для руководства, а не столько на важности собственно технологии<sup>3</sup>. Для каждой информационной системы сначала индивидуально оцениваются важность информации для организации, угрозы и возможные последствия, а затем в целом определяется глобальная степень опасности. Такие оценки являются субъективными и обычно выражаются в терминах высокий, средний и низкий уровень риска,

---

<sup>3</sup> В отличие от метода нисходящей пошаговой детализации, подробные методики, используемые на втором уровне подхода, предлагаемого настоящим Руководством, количественно и очень детально определяют угрозы в отношении компьютерных платформ, на которых работают информационные системы.

последствий и незащищенности.

Исходя из этих оценок, руководство получает рекомендации о дальнейших действиях или о типе определенных средств контроля и мер обеспечения безопасности, которые следует реализовать. Данные рекомендации являются частью управления рисками.

Метод нисходящей пошаговой детализации имеет ряд преимуществ. Он простой и недорогой. Он не механизирован и может быть применен любым высшим органом аудита, в штате которого имеются сотрудники, осведомленные в вопросах средств контроля управления и информационных и компьютерных систем в целом. Внутренних кадровых ресурсов может оказаться достаточно. Нет необходимости в установке сложных пакетов программного обеспечения для сбора данных о проверяемых информационных системах, для получения обновленных и подходящих статистических данных и для выполнения очень сложных анализов и составления отчетов. В случае использования микрокомпьютера обычно достаточно пакета обработки текстов. Электронные таблицы могут помочь в составлении итоговых таблиц. Для получения большего количества преимуществ можно использовать пакеты, которые обеспечивают функциональность баз данных для сбора информации и последующего составления отчетов по результатам анализа.

В предлагаемом двухуровневом подходе к проверке обеспечения безопасности информационных систем метод нисходящей пошаговой детализации рассматривается как точка принятия решения в отношении метода в целом. В зависимости от обстоятельств проверки высшие органы аудита могут быть удовлетворены результатами проверки или могут принять решение о выполнении проверки с применением более сложных процедур в областях особого значения или там, где может потребоваться для руководства привести обоснование введения специальных или дорогостоящих мер обеспечения безопасности.

## **Метод детализации обеспечения безопасности информационных систем - Том 3**

Методики детализации, используемые на втором уровне подхода, предлагаемого высшим органам аудита, представляют собой анализ и управление рисками хорошо известного типа, основанные на подробном и количественном анализе имущества/ресурсов информационных систем. При их помощи измеряются в чисто денежном выражении последствия рисков нарушения безопасности и внедрения контрмер. Производители по всему миру продают различные пакеты анализа безопасности, которые обеспечивают реализацию такого подхода.

Количественные методы анализа обеспечения безопасности обычно доступны вместе с программным обеспечением микрокомпьютера для аудитора, поскольку ввод данных, расчет рисков нарушения безопасности и составление отчетности по проекту могут на практике оказаться длительным и трудоемким процессом. Такие пакеты управления рисками предоставляются поставщиками вместе с экспертной поддержкой и программой обучения пользователей работе с методом. В третьем томе Руководства описывается неавтоматизированная версия метода детализации обеспечения безопасности информации<sup>4</sup>. Задача тома заключается в том, чтобы познакомить высшие органы аудита с методом, который лучше всего используется при поддержке автоматизированного пакета программного обеспечения.

По сравнению с методом нисходящей пошаговой детализации количественный анализ обеспечения безопасности оценивает в денежном выражении подробно и структурировано все имущество/ресурсы и все возможные угрозы и последствия в отношении информационных систем, находящихся в распоряжении организации. Посредством проведения интервью и опросов выполняется оценка возможных последствий для информации пользователями по шкале от одного до десяти в зависимости от

---

<sup>4</sup> Разработано Национальным контрольно-ревизионным управлением Соединенного Королевства.

серьезности таких последствий. Затем рассчитываются показатели ожидаемого ущерба за год путем сложения расходов на замену имущества/ресурсов, вероятностей угроз и весовых коэффициентов последствий.

Большинство методов, имеющих на рынке, относятся ко второму уровню и отличаются друг от друга способом получения значений вероятностей, расходов и определения показателей ожидаемого ущерба за год. Другие различия могут заключаться в удобстве метода для пользователя и типе поддержки, предоставляемой производителем. Указанный двухуровневый подход занимается некоторыми проблемами.

Применение количественных методов анализа и управления рисками требует изменение таблиц статистических данных рисков и стоимости имущества/ресурсов применительно к обстоятельствам каждой отдельно взятой страны.

### **Как применяется двухуровневый подход к проверкам информационных систем**

**Планирование.** Планирование проверки обеспечения безопасности является ключом к успеху. Оно должно охватывать следующие основные элементы:

- Знание клиента и среды;
- Пределы проведения проверки: какие информационные системы, какие логические, физические или географические границы?
- Доступные ресурсы: квалифицированный персонал или консультанты, бюджет, сроки;
- Наличие надежных статистических данных об угрозах и показателей стоимости, соответствующих для местных условий; при необходимости, корректировка значений по умолчанию;
- Требования к отчетности: пользователи отчета, обстоятельства проверки (ежегодный отчет, специальный отчет, внутренний, внешний и т.д.), тип необходимых рекомендаций;

- Метод проверки: метод нисходящей пошаговой детализации, подробный анализ или использование обоих методов.

## **Когда и как применяется метод нисходящей пошаговой детализации в проверке - Том 2**

Лучше всего использовать метод нисходящей пошаговой детализации, поскольку он отвечает потребностям и возможностям многих высших органов аудита.

Том 2 включает описание метода, включая пошаговое выполнение проверки обеспечения безопасности. В приложениях к пакету приводится ряд форм. Формы можно использовать в распечатанном виде или на микрокомпьютере.<sup>5</sup>

К самым важным формам относятся «Сообщение об уязвимости информации и определение категории защиты» (Приложение С) и «Оценка последствий и угроз для деятельности» (Приложение Е). В зависимости от обстоятельств проверки безопасности владельцы/пользователи проверяемых информационных систем могут заполнить печатные копии данных форм, которые подписываются ответственным лицом. Заполненные формы становятся неотъемлемой частью документации оценки обеспечения безопасности данных систем. Наличие этих форм в электронном виде упрощает их изменение в соответствии с локальными потребностями.

Другие формы, в большинстве своем таблицы, используются для объединения результатов по нескольким информационным системам в основную таблицу. Если программа Lotus-1-2-3 не доступна, сотрудник службы безопасности может воспользоваться этими формами и объединить информацию из отдельных оценок обеспечения безопасности в многоколоночных электронных таблицах.

---

<sup>5</sup> Формы разработаны в программе WP 5.1 и Lotus 123 версии 2.01. Формы доступны в электронном виде и их можно легко импортировать в среду Windows.



## **Когда и как применяются методы детализации в проверке обеспечения безопасности информации - Том 3**

Существуют обстоятельства, при которых более детальные с определением количественных показателей проверки обеспечения безопасности информации будут являться стандартом. Это случаи, когда высшие органы аудита располагают бюджетными, техническими и кадровыми ресурсами для проведения такого детального анализа или когда требования к отчетности диктуют применение именно такого подхода.

Перед тем, как использовать метод детализации проверки обеспечения безопасности информации, настоятельно рекомендуется высшим органам аудита обратить внимание на:

наличие экспертной оценки в отношении информационной технологии и обеспечения безопасности информации;

- наличие подходящей методики;
- наличие хорошего вспомогательного пакета программного обеспечения: Количественные методы оценки риска являются в высшей степени комплексными и включают методики детализации, которые «так и просят» использовать микрокомпьютер; но с другой стороны, пакет программного обеспечения микрокомпьютера обычно создает определенные сложности, делая детальные проверки обеспечения безопасности трудноразрешимой задачей;

- бюджет для адаптации пакета или внесения в него изменений согласно желаниям заказчика к проверяемой среде: Нередко на это уходит несколько месяцев работы;

- бюджет на обучение, поскольку кривая обучения может оказаться достаточно крутой и дорогой, особенно если нужно привлекать консультантов;

- временные и финансовые ресурсы: Детальные или количественные проверки обеспечения безопасности, как правило, характеризуются тем, что отнимают много времени и ресурсов; а также

- потребность в такой детальной проверке: Не так давно уже обсуждалось, что детальные количественные проверки обеспечения безопасности не могут считаться обоснованными для коммерческих или государственных информационных систем, которые не являются ни комплексными, ни сильно уязвимыми.

Высшие органы аудита такие, как Национальное контрольно-ревизионное управление Соединенного Королевства и Контрольно-ревизионное управление Новой Зеландии, уже имеют большой опыт в разработке и применении методов детализации управления рисками нарушения безопасности. Те же высшие органы аудита, которые не обладают таким опытом, могут у них проконсультироваться прежде, чем получить подобный опыт.

Для эффективного применения данных методов высшим органам аудита нужно иметь доступ к кадрам или консультантам, которые обладают квалификацией в области информационных технологий И знанием концепций обеспечения безопасности информации. Поскольку коммерческие пакеты управления рисками широко представлены на мировом рынке несколькими консалтинговыми фирмами, то эти же фирмы при продаже пакета предоставляют обучающую программу об использовании базовой методики.

Существует несколько хорошо известных пакетов управления рисками. Например, пакет CRAMM был разработан британским правительством и на сегодняшний день продается во всем мире разными консалтинговыми фирмами. В США хорошо зарекомендовал себя пакет RiskWatch, который использует программное обеспечение системы экспертов для проведения анализа и управления рисками. Министерство энергетики США разработало пакет LosAlamos Vulnerability Assessment (LAVA) (оценка уязвимости Лос-Аламос). Новая Зеландия разрабатывает пакет CATALYST, который работает в среде Windows и отвечает собственным потребностям страны в анализе безопасности. Выбор пакета

определяется его наличием, стоимостью, послепродажной поддержки и количеством изменений, необходимых для использования пакета в местных условиях.

Стоимость одного из коммерческих пакетов для высшего органа аудита равна примерно 6 000 фунтам стерлингам или 10 000 долларам США. Эта стоимость может также включать обучение одного или двух лиц.

В любом случае высшие органы аудита должны удостовериться, что основные статистические данные, используемые выбранным пакетом, подходят их местным условиям. В противном же случае, результаты могут отражать условия, имеющиеся только в Европе или в Северной Америке.

# **Методика проверки обеспечения безопасности информационных систем**

## **Руководство по проверке обеспечения безопасности информационных систем в государственных организациях**

### **Том 2: Метод нисходящей пошаговой детализации**

#### **Сообщение об уязвимости информации и оценка безопасности компьютерных информационных систем**

## **I ВВЕДЕНИЕ**

Настоящее руководство предназначено для обеспечения экономически эффективной методики, которая помогает при проверке или определении подходящих стратегий и мер обеспечения безопасности в пределах организации. Признавая тот факт, что требования к безопасности нуждаются в регулярном обновлении, настоящее руководство также предусматривает простую документацию, обновление и отчетность.

Здесь описывается процедура оценки компьютерной безопасности с точки зрения руководства государственной организации<sup>6</sup>. Организации могут использовать настоящее руководство при составлении «реестра» используемых компьютерных приложений, при оценке уязвимости и присвоении категории защиты информации и при проведении полной оценки безопасности по рискам, угрозам и последствиям для деятельности. Сотрудник, отвечающий за безопасность,<sup>7</sup> использует настоящий документ в качестве основания общей оценки стратегий и мер безопасности и для составления рекомендаций.

Высшими органами аудита руководство может быть использовано для внутренних целей, а именно, для настройки процесса оценки безопасности в своей собственной организации, или для внешних целей - в помощь при проверке процесса оценки безопасности в других государственных организациях.

В данном руководстве рассматривается подход «сверху-вниз» высокого уровня к безопасности информации. Акцент делается на информации, которая передается на различных электронных устройствах. Вместе с этим подходом высокого уровня, настоящее руководство категоризирует угрожающие факторы по общим причинам, а не по результатам, например, землетрясение, а не разрушения, которые оно может

---

<sup>6</sup> Под «организацией» понимается любое правительственное учреждение, агентство или государственная корпорация. В настоящем документе термины «компьютерное приложение» и «информационная система» взаимозаменяемы.

<sup>7</sup> Подробнее о типичной инфраструктуре безопасности в правительстве смотрите Приложение I.

принести. С другой стороны, детальный восходящий подход к безопасности информации рассматривает слабые места каждого возможного компьютерного средства, которые могут создать риск потери информации, сформированной или передаваемой этими средствами. Преимущество использования нисходящего подхода заключается в том, что этот подход помогает руководству быстро переключиться и сфокусироваться на проблемных зонах для определения дальнейших действий. В некоторых случаях этот подход может указать на необходимость более детальной работы с целью построения экономической модели масштабных или дорогостоящих мер обеспечения безопасности.

Так как метод всегда принимает взгляд организации или руководства на информационную безопасность, он всегда остается гибким и может решать вопросы политики по безопасности, а также мер безопасности.

## **II ПРОЦЕСС ОЦЕНКИ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ**

### **Эволюция управления информацией**

В управлении информацией и приложениями организация проходит через четыре четко выраженных этапа: управление разработкой документации, управление автоматизированными технологиями, управление корпоративными информационными ресурсами и, наконец, управление стратегическим использованием информации (Приложение А). Основные задачи в отношении технологий и безопасности заключаются в минимизации времени и усилий, затрачиваемых на каждом этапе, и в максимально возможном ровном переходе с одного этапа на другой.

На этапе управления автоматизированными технологиями пользователи несильно полагаются на компьютерные приложения, но достигают заметной эффективности. На третьем этапе, а именно, этапе управления корпоративными информационными ресурсами, компьютерная безопасность становится главной задачей в связи с значительной

зависимостью от компьютеризированной информации и в связи с рисками, связанными с концентрацией информации в одном месте.

### **Управление безопасностью**

Одним из ключевых ресурсов Организации является ее информация. Первым шагом в обеспечении безопасной обработки данных является адаптация информации и административных стратегий управления и мер, которые включают принципы эффективного управления безопасностью.

1. Защита безопасности должна соответствовать важности защищаемой информации;
2. Защита безопасности должна контролировать информацию каждый раз при ее перемещении или обработке; а также
3. Защита безопасности должна быть постоянной во всех ситуациях.

### **Служба безопасности**

Под руководством лица, отвечающего за компьютерную безопасность, создается служба безопасности. Полная заинтересованность высшего руководства крайне важна для того, чтобы служба могла достичь своих целей. Служба отвечает за внедрение политики безопасности, определяемой высшим руководством, и за идентификацию изменений, необходимых в связи с доработками информационных систем организации или в связи с угрозами, которые на них направлены.

### **Процесс**

Стратегии безопасности созданы для защиты информации в соответствии с рисками информации. Меры безопасности (стандарты, процедуры и инструменты) представляют собой стандартные блоки защиты информации.

При определении необходимых конкретных мер следует соблюдать процесс оценки компьютерной безопасности (Приложение В), который включает:

- **Сообщение об уязвимости:**

оценка уязвимости программных и административных приложений (информационных систем), используемых в Организации, и определение категории защиты;

подтверждение стандартной оценки Организации похожих приложений и, по возможности, заполнение или обновление формы «Сообщение об уязвимости информации и определение категории защиты» (Приложение С);

накапливание отдельных сообщений об уязвимости для составления краткого описания информационных систем (Приложение D) там, где необходимо.

- **Оценка последствий для деятельности:**

Определение возможного воздействия на деятельность Организации в случае раскрытия информации, риска сохранности или прекращения обслуживания.

- **Оценка угроз и рисков:**

определение риска (вероятности), что идентифицированные угрозы могут произойти.

- **Оценка уровня риска нарушения безопасности:**

оценка последствий и угроз для деятельности вместе с определением влияния на Организацию в целом;

подтверждение стандартной оценки Организации обеспечения безопасности похожих приложений и, по возможности, подтверждение или обновление формы «Оценка последствий и угроз для деятельности» (Приложение E);

- **Решение по обеспечению безопасности и рекомендуемые мероприятия:**

заполнение или обновление формы «Сводная информация по оценкам обеспечения безопасности» (Приложение G);

принятие решений по обеспечению безопасности и предложение мероприятий руководству для минимизации идентифицированных рисков



нарушения безопасности, а также озвучивание какого-либо серьезного недостатка политики безопасности.

### **III ЗАПОЛНЕНИЕ ФОРМЫ «СООБЩЕНИЕ ОБ УЯЗВИМОСТИ ИНФОРМАЦИИ И ОПРЕДЕЛЕНИЕ КАТЕГОРИИ ЗАЩИТЫ»**

Для проведения проверки важно составить полный «реестр» всех операций и административных приложений (по группам или по отдельности), которые используются, и точно обозначить границы проверяемой (ых) системы (систем). Определение термина «приложение» приводится в Приложении I. **В целях безопасности, похожие приложения можно сгруппировать, например, работа с текстом Letters (Письма), работа с текстом Audit Memorandums (меморандумы по аудиту), динамические таблицы Financial Analysis (финансовый анализ), динамическая таблица Planning Schedule (график планирования) и т.д.**

Приложения принадлежат либо к какой-либо группе, либо лицу. В случае малого взаимодействия между приложениями можно без труда установить пользователей выходных данных системы. В высоко интегрированных системах искусственная граница должна быть согласована всеми сторонами, включая высшее руководство.

Группа может попросить членов заполнить форму сообщения об уязвимости пользовательской информации и категории защиты (Приложение С), чтобы составить «реестр» приложений, которые используются, и собрать данные, необходимые для объединения похожих приложений. Форма должна быть проверена и утверждена руководителем группы. Эти действия гарантируют, что все оценки отражают истинное значение информационной системы для организации в целом.

При заполнении формы сообщения об уязвимости информации и категории защиты (Приложение С) владелец оценивает уязвимость информации с точки зрения доступности, сохранности и

конфиденциальности, оценивает расходы на замену и скрытые издержки, прямые и косвенные издержки (коэффициент часов к среднему курсу доллара и расходы) и определяет необходимую категорию защиты.

Форма «Сообщение об уязвимости информации и определение категории защиты» представляет собой официальный документ оценки. Форма также помогает документально зафиксировать определенные средства контроля целостности и процедуры (полноты, точности и авторизации). Данный документ хранится как текущая документация и обновляется по мере необходимости.

В случае необходимости и при окончательном оформлении отдельные сообщения об уязвимости накапливаются руководством на уровне группы или на уровне организации для составления краткого описания информационных систем (Приложение D). Таким образом руководство получает общее представление о системах, за которые оно отвечает, и о важности информации, которая в них содержится.

#### **IV ЗАПОЛНЕНИЕ ФОРМЫ «ОЦЕНКА ПОСЛЕДСТВИЙ И УГРОЗ ДЛЯ ДЕЯТЕЛЬНОСТИ»**

Форма «Оценка последствий и угроз для деятельности» (Приложение E) обеспечивает структурированную оценку уровня рисков нарушения безопасности для Организации. Оценка состоит из трех компонентов: риск (вероятность) появления угрозы, степень серьезности последствий для деятельности и оценка уровня риска нарушения безопасности. Первые два компонента не зависят друг от друга, и их оценку можно выполнить в любом порядке. Затем одновременно оцениваются последствия и угрозы для деятельности с целью получения общей оценки уровня риска нарушения безопасности Организации.

##### **Оценка угроз и рисков**

Угроза - это то, что может случиться. Перечень возможных угроз приводится в Приложении E. Более подробный перечень с предлагаемыми

контрмерами приводится в Приложении Н. Согласно исследованиям обеспечения безопасности, более 80% угроз в отношении компьютерной информации происходит в пределах организации (совершается инсайдерами), причем 24% из-за невнимательности к процедурам (небрежности), 26% по причине недостаточной подготовки сотрудников и 30% из-за непорядочности сотрудников.

Следует уделить внимание локальным условиям, в которых характер и значительность угроз могут сильно отличаться для разных стран. В некоторых случаях это может означать необходимость больше сфокусироваться на определенных типах угроз, определении некоторых угроз и корректировке контрмер к местным условиям.

Вероятность появления - это шанс, что угроза появится. Поскольку некоторые угрозы и риски могут оказаться общими для всей организации, лицо, отвечающее за компьютерную безопасность, должно составить общую оценку и использовать ее как критерий проведения индивидуальных оценок. Лицам, дающим свои оценки, нужно сконцентрироваться только на рисках, которые релевантны или могут отличаться в силу особых обстоятельств. Для каждой информационной системы вероятность появления определенных угроз оценивается как высокая, средняя или низкая. После того, как идентифицированы и оценены все возможные угрозы для приложения, осуществляется оценочное суждение по общему риску. Для данной информационной системы риск в целом не является результатом сложения высоких и низких оценок уровня риска. Единичная оценка высокого уровня в критической области может привести к высокому уровню риска в целом. С другой стороны, несколько оценок высокого уровня в некритических областях могут привести к среднему или низкому уровню риска в целом.

### **Оценка последствий для деятельности**

Для выполнения данной оценки нужно принять бизнес-решения в отношении важности информации. В целях обеспечения безопасности показатели ценность деятельности выражаются в виде последствий для

деятельности Организации в случае раскрытия информации, риска ее сохранности или прекращения обслуживания. Перечень возможных последствий для деятельности приводится в Приложении Е. В зависимости от местных условий можно определить другие возможные последствия для деятельности. В отношении каждого последствия для деятельности принимаются решения, которые определяют степень серьезности последствий, если таковые имеют место. Последствия могут быть очень серьезными, серьезными или несущественными. Выполняется оценка только тех последствий для деятельности, которые связаны с информацией. После оценки всех возможных последствий дается оценка последствий для бизнеса в целом в отношении приложения.

Каждая из этих оценок – субъективное оценочное суждение по серьезности каждого отдельного фактора воздействия на организацию в целом. Таким же образом, после оценки отдельных последствий для организации в случае раскрытия информации, нарушения ее безопасности или когда информация становится недоступной, дается оценка последствий для деятельности в целом, но не на основе точного нарастающего итога этих отдельных последствий, а на основе оценочного суждения относительно общего эффекта, оказанного на организацию. Данные оценочные суждения формируются посредством достижения консенсуса между различными ключевыми заинтересованными сторонами.

Оценки последствий для деятельности и рисков угроз считаются приемлемым только после того, как с ними ознакомятся и утвердят руководитель организационной группы и лицо, отвечающее за компьютерную безопасность.

### **Оценка уровня риска нарушения безопасности**

Оценка уровня риска нарушения безопасности представляет собой результат объединения степени или вероятности (высокая, средняя, низкая) риска угроз в целом и общего показателя последствий для деятельности (очень серьезный, серьезный или несущественный). Таблица оценки уровня

риска Приложения F используется в качестве справочной таблицы для определения высокого, среднего и низкого уровня риска нарушения.

Сначала дается общая оценка риска нарушения для приложения в целом по форме «Оценка последствий и угроз для деятельности» (Приложение E).

Например, в случае высокой оценки общего риска угроз (вертикальная ось), но при низком уровне последствий в целом для деятельности (горизонтальная ось) по таблице оценки уровня рисков на пересечении осей получаем значение «4». Это означает средний уровень риска нарушения безопасности. Подробнее о перераспределении оценок риска нарушения безопасности в группы низкого, среднего или высокого уровня смотрите условные обозначения в таблице оценки уровня рисков или в таблице Раздела VI настоящего руководства.

Затем, для определения того, на какой риск угроз и последствия для деятельности следует обратить внимание руководству в первую очередь, рассчитывается оценка уровня риска нарушения безопасности в отношении этих последствий для деятельности, получивших оценку. Расчет выполняется при помощи таблицы оценок уровня риска, которая помогает объединить оценку отдельного последствия для деятельности и установленный риск угроз в целом. Цифры, полученные из таблицы оценок уровня риска, вносятся в соответствующие строки последствий, в область оценки риска нарушения безопасности формы E. Для большей ясности, цифры записываются в соответствующих колонках Hi (высокий), Med (средний) или Lo (низкий). Средний или высокий уровень риска нарушения безопасности могут стать объектом рекомендаций, предоставляемых руководству, по переоценке последствий для деятельности или по снижению риска угроз в целом, чтобы уменьшить риск нарушения безопасности для организации.

Данная оценка представляет собой связующее звено между рисками нарушения безопасности и тем, какие решения по обеспечению безопасности

и меры необходимо предпринять.

## **V СВОДНАЯ ИНФОРМАЦИЯ ПО ОЦЕНКАМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ**

Форма «Сводная информация по оценкам обеспечения информации» (Приложение G) объединяет информацию, собранную и прошедшую оценку в формах «Сообщение об уязвимости информации и определение категории защиты» (Приложение C) и в формах «Оценка последствий и угроз для деятельности» (Приложение E). Выполняется подготовка сводных сведений по группам с разделением операций по выполнению программ и административной работы. Данные формы и сводные сведения должны храниться как рабочие документы и регулярно обновляться. Они должны быть представлены на рассмотрение и утверждены соответствующим руководителем.

Сводные сведения дают представление высшему руководству об обеспечении безопасности используемых приложений. Исходя из сводных сведений и оценок приложений, лицо, отвечающее за компьютерную безопасность, оценивает риски нарушения безопасности Организации и дает рекомендации относительно мероприятий, которые необходимо провести для минимизации установленных рисков нарушения безопасности. При изменении характера технологии процесс проверки рисков может также выявить стратегии безопасности, которые больше не подходят для использования. Все серьезные недостатки стратегии доводятся до внимания высшего руководства в окончательном отчете вместе с другими рекомендациями. Если для конкретной программы или информационной системы результаты показывают необходимость составления более точных рекомендаций, то можно рекомендовать провести более детальную проверку, используя тщательный количественный анализ, чтобы определить, какие контрмеры для обеспечения безопасности необходимо предпринять, или для оценки возможных альтернатив.

В целях оценки обеспечения безопасности и схематизации приоритетов оценка уровня угроз и рисков, последствий для деятельности и их ранжирование в случае появления угрозы, и, наконец, общая оценка организационного риска нарушения безопасности очень помогают в составлении приемлемых долгосрочных планов по обеспечению безопасности.

## **VI РЕШЕНИЕ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ И РЕКОМЕНДУЕМЫЕ МЕРОПРИЯТИЯ**

Касательно оценки каждого риска нарушения безопасности (форма «Оценка последствий и угроз для деятельности») принимается решение по обеспечению безопасности и даются рекомендации относительно действий руководства. Связь между риском нарушения безопасности и решением по обеспечению безопасности и рекомендуемыми мероприятиями представлена в таблице ниже.

Уровень риска нарушения безопасности	Решение по обеспечению безопасности	Рекомендуемое мероприятие
ВЫСОКИЙ (9,8,7)	Контроль риска	Внедрить дополнительные стратегии и принять меры (стандарты, процедуры, инструменты)
СРЕДНИЙ (6,5,4)	Контроль риска Избегание риска	Внедрить дополнительные стратегии и принять меры Изменить / улучшить последовательность операций
НИЗКИЙ (3,2,1)	Избегание риска	Изменить / улучшить последовательность операций
	Ограничение риска Принятие риска	Получить страховое покрытие Никаких изменений / продолжать работу согласно плану

Если необходимо рекомендовать определенные меры, в Приложении Н приводится полный перечень проводимых возможных мероприятий. Наряду с профессиональным мнением и оценкой издержек перечень может служить основанием для рекомендации определенных средств контроля и мер обеспечения безопасности.

После проверки лицом, отвечающим за компьютерную безопасность, отчет об обеспечении безопасности и рекомендации передаются высшему руководству через Руководящий комитет по информационным системам для

принятия дальнейших действий.

## **VII ШАГИ ОЦЕНКИ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ**

Шаги по оценке компьютерной безопасности – отчет по уязвимости информации и категории защиты, оценка воздействия на деятельность, оценка рисков и угрожающих факторов, оценка показателей риска и решения по безопасности/рекомендуемые действия – указаны в Приложении В. Эти шаги включают:

1 Каждая организационная группа оценивает уязвимость информации своих приложений и определяет категорию защиты

или

подтверждает содержание формы «Сообщение об уязвимости информации и определении категории защиты» и, при необходимости, обновляет форму, а также должным образом получает ее одобрение.

Приложение С. Сообщение об уязвимости информации и определение категории защиты -форма

Приложение D. Краткое описание информационных систем -электронная таблица<sup>8</sup>

2 В отношении своих приложений организационная группа оценивает последствия для деятельности, угрозы и риски

или

подтверждает содержание формы «Оценка последствий и угроз для деятельности» и, при необходимости, обновляет форму, а также должным образом получает ее одобрение.

Приложение E. Оценка последствий и угроз для деятельности -электронная таблица

Приложение F. Таблица оценки уровня риска нарушения безопасности

---

<sup>8</sup> Несмотря на то, что данные формы разработаны как шаблоны электронных таблиц программы Lotus 1-2-3, их легко можно использовать в распечатанном виде или составить вручную.



3 Организационная группа сводит в единую таблицу информацию об оценках обеспечения безопасности используемых приложений согласно предоставленному формату.

Приложение Г. Сводная информация по оценкам обеспечения безопасности -электронная таблица

4 Организационная группа отправляет копию сводной информации и две формы сотруднику, отвечающему за компьютерную безопасность, для проверки и, при необходимости, встречается с ним для окончательного оформления отчета оценки безопасности.

Приложение Г. Сводная информация по оценкам обеспечения безопасности - электронная таблица

Приложение С. Сообщение об уязвимости информации и определение категории защиты - форма

Приложение Е. Оценка последствий и угроз для деятельности - электронная таблица

5 Сотрудник, отвечающей за компьютерную безопасность, утверждает сводную информацию и, если необходимо, эта информация проверяется и утверждается директором службы безопасности.

Приложение Г. Сводная информация по оценкам обеспечения безопасности - электронная таблица

6 Окончательная сводная информация проверяется и утверждается руководителем, ответственным за организационную группу.

Приложение Г. Сводная информация по оценкам обеспечения безопасности - электронная таблица

7 Сотрудник, отвечающей за компьютерную безопасность, принимает, при необходимости, решения по обеспечению безопасности и определяет рекомендуемые к проведению руководством мероприятия, предназначенные минимизировать идентифицированный(ые) риск(и) нарушения безопасности, и отчитывается перед начальником службы безопасности.

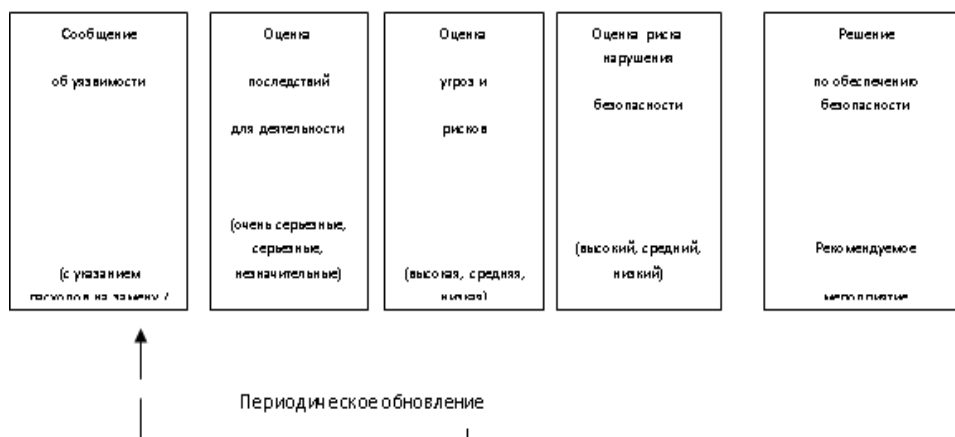
## ПРИЛОЖЕНИЕ А

### ЭВОЛЮЦИЯ УПРАВЛЕНИЯ ИНФОРМАЦИЕЙ

Результаты деятельности в целом



# **ПРИЛОЖЕНИЕ В** **ПРОЦЕСС ОЦЕНКИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ** **ИНФОРМАЦИОННЫХ СИСТЕМ**



Разработанная схема процесса

# ПРИЛОЖЕНИЕ С

## СООБЩЕНИЕ ОБ УЯЗВИМОСТИ ИНФОРМАЦИИ И ОПРЕДЕЛЕНИЕ КАТЕГОРИИ ЗАЩИТЫ

### Введение

Настоящий документ можно использовать в распечатанном виде или как документ WP 5.1 в зависимости от обстоятельств.

При проверке безопасности информационных систем по принципу сверху-вниз настоящий документ используется на этапе анализа рисков для документирования сведений об информационных системах. На каждую систему заполняется отдельная форма.

Приложение: \_\_\_\_\_ Дата: \_\_\_\_\_

(допустимо группирование похожих приложений)

Новый отчет \_\_\_\_\_ Отчет с поправками \_\_\_\_\_

Компьютерная среда:

Микро \_\_\_\_\_ Мини \_\_\_\_\_ Мейнфрейм \_\_\_\_\_ Бюро  
обслуживания \_\_\_\_\_

Используемое программное обеспечение: \_\_\_\_\_

1. Название филиала и, при необходимости, Группы, отвечающей за информацию (т.е. ВЛАДЕЛЕЦ)

Филиал: \_\_\_\_\_ Группа: \_\_\_\_\_

2. Если приложения отнесены в «группу», пропустите пункт «Общее число транзакций». Если возможно, дайте общее описание приложения, включая источник информации, объемы и сложность в обработке.

Объемы		Источники информации	
% от всей организационной информации		Программа заказчика или	
		внешняя программа	/

Общее число транзакций или денежное выражение транзакций  Размер файла  Число записей		управление операциями	
Общее описание приложения и сложности обработки данных			

3. Укажите основную цель и любые вторичные цели информации:

Услуги населению \_\_\_\_\_ Административная функция

Принятие решений \_\_\_\_\_ Финансовая функция

4. Каковы последствия случайного или намеренного изменения

и/или уничтожения информации? ДОСТУПНОСТЬ, ЦЕЛОСТНОСТЬ

Убыток, потеря или повреждение	Да / Нет	Убыток, потеря или повреждение	Да / Нет
<b>Раскрытие / Сохранение целостности информации</b> 1. Затруднения для организации		<b>Сбои в оказании услуг</b> 1. Просрочка выплат по счетам / заработной платы	
2. Потеря доверия к организации		2. Неспособность производить сборы	
3. Компрометация конфиденциальных данных об организации		3. Сбои в обслуживании Правительства	
4. Компрометация данных о заказчиках или третьих лицах		4. Сбои в оказании услуг населению	
5. Компрометация персональных данных		5. Сбои в работе внутренней службы	

6. Компрометация информации государственной важности			
7. Правовые последствия / ответственность за компенсируемые и разрушающие повреждения			

5. Существуют ли процедуры восстановления информации на случаи возникновения чрезвычайных обстоятельств? ДОСТУПНОСТЬ, ЦЕЛОСТНОСТЬ

Процедуры восстановления	Да / Нет	Неизвестно	Комментарии
Резервное копирование			
Внесистемное ЗУ			
Другие методы			

6. Укажите максимальный период восстановления, который Организация может выдержать без доступности приложения или услуги (если имеются определенные ограничения, укажите их). ДОСТУПНОСТЬ

Часов \_\_\_\_ Дней \_\_\_\_ Недель \_\_\_\_ Месяцев \_\_\_\_

Комментарий:

7. Укажите степень важности информации.

(5: Очень важная; 4: Важная; 3: Требующая защиты; 2: Требующая небольшого уровня защиты; 1: Не требующая защиты)

Доступность \_\_\_\_ Целостность \_\_\_\_ Конфиденциальность \_\_\_\_

8. Оцените расходы на замену и скрытые издержки связанные с потерей информации, как прямые, так и косвенные (время, расходы)

Расходы на замену	Человеко-часы	Расходы
Прямые (время, затрачиваемое на восстановление / формирование информации, аппаратных средств и программного обеспечения)		

Непрямые (например, задержки, вызванные выполнением других задач; другие стороны, вовлеченные в восстановление; упущенные из-за потерянной информации возможности и т.д.)		
---	--	--

9. Укажите категорию / обозначение защиты информации для данного приложения / информационной системы:

% информации

\_\_\_\_\_ базовые стандарты защиты (необозначенной информации)

\_\_\_\_\_ защищенной (обозначенной информации)

\_\_\_\_\_ классифицированной информации

\_\_\_\_\_ 100%

Форму заполнил: \_\_\_\_\_ Филиал/Группа: \_\_\_\_\_

Владелец информации

(например, управляющий директор) Утвердил \_\_\_\_\_ Дата: \_\_\_\_\_

Служба безопасности\_ Утвердил \_\_\_\_\_ Дата: \_\_\_\_\_

## ПРИЛОЖЕНИЕ F

### ТАБЛИЦА ОЦЕНКИ УРОВНЯ РИСКА НАРУШЕНИЯ БЕЗОПАСНОСТИ

Последствие Вероятность	Очень серьезное	Серьезное	Несущественное
ВЫСОКАЯ	9	8	4
СРЕДНЯЯ	7	6	3
НИЗКАЯ	5	2	1

(Таблица разработана Королевской Канадской конной полицией)

Уровень риска нарушения безопасности: Высокий (9,8,7)      Средний (6,5,4)      Низкий (3,2,1)



## **ПРИЛОЖЕНИЕ Н**

### **ИСХОДНЫЕ УГРОЗЫ И МЕРЫ БЕЗОПАСНОСТИ**

Настоящий документ содержит перечень угроз и контрмер в отношении имущества/ресурса. Данные угрозы часто представляют собой имеющиеся слабые места, образовавшиеся в результате определенных угроз. Контрмеры представляют собой средства контроля или меры безопасности, которые можно использовать для корректировки или минимизации недостатка безопасности.

В тексте упоминание дисциплинарных мер как возможной меры противодействия или сдерживающего средства против несоответствующих действий сотрудников следует воспринимать в более широком контексте. Дисциплинарные меры должны быть предусмотрены или использованы только если другие меры, такие как осведомленность и обучение, не смогли предотвратить неприемлемые действия или поведение. Эффективными решениями по обеспечению безопасности являются те решения, которые персонал охотно поддерживает.

В конце перечня для всего имущества/ресурсов или предметов, для которых были приведены угрозы и контрмеры, составлен алфавитный указатель.

В тексте для каждого ресурса/объекта имущества используются следующие символы:

У = угроза

К = контрмера (средство контроля или мера обеспечения безопасности)

#### **Оглавление приложения Н**

Аппаратные средства	44
Связь	44
Телефонные линии	44

Порты ввода/вывода	44
Модемы	45
Электронная почта	45
Электронные доски объявлений	46
Почтовые услуги	46
Прокладка сетевого кабеля	46
Компьютеры	47
Терминалы	47
Микрокомпьютеры	48
Бездисковые автоматизированные рабочие места	50
Файловые серверы	50
Миникомпьютеры и мейнфрейм	50
Ввод данных	51
Сканеры	51
Вывод данных	51
Общие положения	51
Разделитель-сортировщик	51
Упаковщик	52
Лазерный принтер	52
Устройство контактной печати	53
Устройство графического ввода	53
Очереди вывода документов на печать	53
Дисплей	54
Фотокопировальное устройство	54
Пишущая машинка	54
Хранение	54
Бумажные копии документов	55
Съемные магнитные носители	55
Несъемные магнитные носители	55
Съемные оптические носители	56
Несъемные оптические носители	57
Микрофильм / микрофиша	58
Люди	58
Персонал	59
Угрозы общего характера	59
Ключевой персонал	59
Ввод данных	60
Запросы	61
Обращение с распечатанными документами	61
Программисты	61
Аналитики	62
Системная поддержка	63
Системные программисты	64
Контроль внесения изменений	65
Программисты, отвечающие за библиотеку носителей	65

Логический контроль доступа	66
Физический контроль доступа	66
Аудиторы	67
Владельцы данных	67
Пользователи данных	67
Хранители данных	67
Подрядчики	68
Обслуживание	69
Консультанты	69
Посторонние лица	69
Посетители	69
Злоумышленники	69
Здания	70
Территория организации	70
Ключевые помещения	70
Ввод / обновление данных	72
Обработка	72
Печать	72
Хранение	73
Запросы	74
Связь	74
Операции актуальных прикладных систем	75
Разработка приложений	76
Функции систем	76
Электроэнергетическая установка	77
Бланки для документов	77
Приготовление пищи / курение	78
Ценные бланки для документов	78
Документация	78
Программное обеспечение	79
Аппаратные средства	80
Процедуры	80
Аварийный план	80
Планы этажей	81
Схемы кабельных соединений	81
Словарь данных	82
Условия эксплуатации	82
Кондиционирование воздуха	82
Электропитание	82
Вода	82
Освещение	82
Отходы	83
Бумага	83
Магнитные носители	83
Оптические носители	84

## **Связь**

### **Телефонные линии**

У Телефонные линии могут оборваться или потеряться.

К Провести запасные линии для основных соединений.

У Телефонные линии могут отключить.

К Использовать, где возможно, частные линии.

Избегать прокладки основных линий через зоны общественного пользования.

Избегать направления основных линий через общественные места.  
Рассмотреть использование герметизированных кабельных проводов.

Убедиться, что кабели остаются под землей.

Избегать того, чтобы провода были видны, путем отдельного направления или маркировки

В случае маркировки телефонных линий маркировать все линии связи, а не только основные.

Попробовать использовать шифрование для передачи важной информации. Рассмотрите использование шифровки для передачи секретной информации. Если вы используете шифровку, соблюдайте следующее:

Шифруйте ключи, так же как и данные.

Используйте алгоритм шифровки, соответствующий промышленным стандартам. Рассмотрите использование «разовых» ключей для ограничения полезности раскрытия хотя бы одного ключа.

Используйте несловесные ключи из 6 или более символов.

### **Порты ввода/вывода**

У При изменении соединений портов можно получить контроль над функциями.

С Разместить соединительные коробки в охраняемых зонах, если вы полагаетесь на разрешенные функции для терминалов (компьютеров),

присоединенных к определенным портам.

### **Модемы**

У Модемы можно использовать для получения несанкционированного доступа к системе.

К Не подключать модемы к наборным линиям. Если существует потребность в наборной функции, обеспечить доступ только к центральному узлу, который защищен мощным брандмауэром. Ограничить доступ гостя к особо специфическим приложениям в пределах защищенной среды. Обеспечить гостю сеансы работы с «терминалом», а не сеансы взаимодействия с «хостом» или сеансы с удаленным доступом, поскольку такие сеансы могут открыть доступ к секретной информации на микрокомпьютере или в сети. Попробовать использование шифрования передачи и хранения секретных данных.

Функции обратного вызова обычно слишком ограничивают аудиторов, постоянно передвигающихся на местности, и могут вызвать административную головную боль.

У Модемы можно использовать для несанкционированной передачи информации за пределы организации.

К Свести количество модемов к минимуму; отслеживать использование линий, к которым прикреплены модемы; отключать модемные линии в нерабочие часы.

### **Электронная почта**

У Электронную почту можно использовать для несанкционированной передачи информации за пределы организации.

К Сохранять копии всех отправленных электронных писем и вести учет отправителя и получателя.

Осуществлять выборочные проверки содержимого электронной почты.

Использовать программы поиска для обнаружения ключевых слов в электронных письмах.

Вносить в таблицы отправителей и получателей для установления

любых подозрительных связей.

(Предупреждение: В некоторых странах перехват сообщений электронной почты может быть незаконным или регулироваться специальным законодательством.)

### **Электронные доски объявлений**

У Электронные доски объявлений можно использовать как средство передачи информации за пределы организации.

К Направляйте все соединения с досками объявлений через центральный пункт. Используйте автономные считывающие устройства для извлечения сообщений и ответов по почте. Это позволит вам контролировать трафик на доски объявлений и с них таким же образом, как и электронную почту.

У Вредоносное программное обеспечение, содержащее вирусы или троянские программы, может быть получено через электронные доски объявлений

К Все запросы на загрузку файлов с досок объявлений должны направляться через центральное отделение специалистов. Загружаемые файлы должны досконально проверяться на вирусы и т.д.

### **Почтовые услуги**

У Вредоносное программное обеспечение обнаруживается на дисках, отправляемых по почте.

К Ввести процедуру, согласно которой будет вводиться дисциплинарное взыскание для каждого, кто будет использовать диск перед проверкой сотрудниками технической поддержки

У Почтовую службу можно использовать для передачи информации за пределы организации.

К Регистрировать документы и диски, которые содержат секретные материалы, и ввести процедуры контроля их копирования.

### **Прокладка сетевого кабеля**

У На сетевые кабели может быть установлено подслушивающее

устройство для перехвата информации или внедрения незаконных сообщений

**К** Не допускать прокладку сетевых кабелей через общедоступные зоны. Попробовать использование запираемых кабельных лотков. Всегда проверять длину кабелей, которые только что обслуживались техническими специалистами. Использовать шифрование разделов сети, которые содержат секретную информацию.

**У** В случае разрыва одной из секций кабеля в работе сетей может произойти сбой.

**К** Разработать сеть для минимизации последствий сбоя любой секции кабеля. Рассмотреть дублирование проводов для основных соединений.

### **Компьютеры**

#### **Терминалы**

**У** Несанкционированный доступ к данным можно получить с клавиатуры микрокомпьютера или любого терминала в сети.

**К** Операционная система и программное обеспечение должны использовать процедуры идентификации и аутентификации для обеспечения гарантии того, что запросы доступа осуществляются от авторизованных лиц. Все действия, которые могут оказывать материальный эффект на деятельность, должны фиксироваться в журнале. Одновременное применение процедур идентификации, аутентификации и входа в систему является основой системы контроля и учета пользователей.

В случае использования паролей для аутентификации пароли должны состоять из 6 или более символов и должны быть удобопроизносимыми, но не в виде слов. Лучше всего, если компьютер сам генерирует пароли во избежании выбора обычного или дублирующего пароля. В случае использования паролей, сгенерированных компьютером, важно, чтобы они были удобопроизносимыми, т.е. человек мог их запомнить не записывая.

По возможности попробуйте использовать единый пароль для каждого

лица. Несколько паролей труднее запомнить, в результате чего люди будут их записывать, что является нарушением безопасности.

Пароли должны регулярно меняться. Чем большую важность представляют функции, к которым пароли предоставляют доступ, тем чаще нужно менять пароли. Для ключевых транзакций оправданно использование только разовых паролей. Причина для смены паролей и шифровальных ключей часто заключается в снижении ущерба от раскрытия пароля несанкционированным лицом.

У Терминал, который оставлен пользователем, не выполнившим выход из системы, представляет возможность для любого лица притвориться оператором, который вошел в систему.

К Процедуры должны предусматривать дисциплинарное взыскание за оставленный без присмотра подключенный терминал. Операционная система / программное обеспечение должно обеспечивать выход терминалов из системы по истечению короткого периода бездействия на терминале или автоматическую блокировку терминала так, чтобы любая дальнейшая деятельность на данном терминале требовала повторного ввода данных идентификации и аутентификации.

У Важные данные могут быть изменены через любое местное или модемное соединение с информационной системой.

К Контроль идентификации и опознавания несколько снижает риск несанкционированных изменений важных данных. Изменения основных данных должны подлежать подтверждению контролирующим лицом в дополнение к обычным проверкам.

### **Микрокомпьютеры**

У Микрокомпьютеры легко украсть.

К Маркировать все микрокомпьютеры и периферийные устройства несмываемой краской. Хранить инвентарную опись всех микрокомпьютеров и периодически проверять ее. Покупать микрокомпьютеры с блокировкой, которая отключает клавиатуру, и со съемным корпусом.



Внедрить систему регистрации компьютеров, которые заносятся в здание и выносятся из него. Охранники должны быть проинструктированы об обязанности проводить выборочные проверки, чтобы удостовериться, что персонал не выносит с собой компьютеры, периферийные устройства или расходные материалы за пределы здания без разрешения.

Устанавливать микрокомпьютеры так, чтобы их было не видно из зон общественного пользования.

У Микрокомпьютеры могут стать недоступными в случае потери их ключей.

К Хранить один из ключей от каждого микрокомпьютера в запортом на ключ кабинете отдела материально-технического обеспечения.

У Микрокомпьютеры особенно подвержены воздействию вредоносного ПО, вирусов, троянов, поскольку пользователь может легко копировать программы в компьютер, используя гибкие диски. Вредоносное ПО может быть также занесено неумышленно с гибких дисков из неконтролируемых сред и со средств распределения, таких как коробочное ПО и CD-ROM.

К Ввести процедуру, согласно которой использование любой программы на микрокомпьютере до прохождения ей тестирования в службе поддержки считается дисциплинарным нарушением. Обеспечить частое резервное копирование важных данных и важного ПО. Служба поддержки должна вести учет ПО, разрешенного к использованию на каждом компьютере, и проводить выборочные проверки, чтобы убедиться, что сотрудники не пользуются неразрешенным ПО.

Принять специальные меры предосторожности по отношению к CD-ROMам, так как они могут быть заражены вирусами, как и любой другой носитель, но их нельзя очистить.

У Микрокомпьютеры обычно чувствительны к сбоям.

К Подготовить и проверьте аварийные планы для работы со сбоем любого микрокомпьютера, который поддерживает важнейшие функции.

У Микрокомпьютеры используются и обслуживаются скорее пользователями, чем специалистами. Поэтому необходимости резервного копирования и обеспечения безопасности часто не уделяется должного внимания.

К Купить ленточные накопители для машин, используемых для хранения больших объемов временной информации.

Внедрить процедуры, информировать и провести обучение сотрудников с целью разъяснения необходимости выполнения резервного копирования информации, должного обращения с оборудованием и обеспечения безопасности данных.

У Микрокомпьютеры можно использовать для загрузки незаконных программ в сети, потому что у них есть разъемы для гибких дисков.

К Позволяйте передачу файлов в сеть только когда это важно. Запретить передавать «выполняемые» файлы. Внедрить процедуры, согласно которым перенос программ пользователями в или из сети считается дисциплинарным нарушением. Использовать бездисковые автоматизированные рабочие места, если в использовании гибких дисков для работы сотрудника нет необходимости.

### **Бездисковые автоматизированные рабочие места**

У Местоположение автоматизированных рабочих мест можно изменять.

К Если имеющаяся система контроля доступа исходит из разрешенных функций для конкретных терминалов (компьютеров), тогда необходимо внедрить процедуры, которые лишают пользователей прав в случае изменения места расположения их компьютеров. В противном случае существует риск переноса компьютера из безопасной зоны в небезопасную.

### **Файловые серверы**

У Сбой работы компьютера может привести к недоступности системы.

К Внедрить процедуры резервного копирования и стратегию восстановления в случае отказа файлового сервера. Резервное копирование должно обеспечивать, по крайней мере, три генерации на рабочем месте и одну генерацию вне рабочего места. Характер и частота резервных копий изменяются пропорционально важности приложений, поддерживаемых файловым сервером. Во многих случаях нормой является еженедельное полное резервное копирования и ежедневное инкрементное резервное копирование. Автоматическое резервное копирование можно выполнять в нерабочие часы, когда полное резервное копирование проходит также легко как и инкрементное.

Дублирование хранения и обработки может быть необходимо для файловых серверов, которые поддерживают важнейшие приложения.

#### **Миникомпьютеры и мейнфрейм**

У Сбой компьютера может повлиять на многих пользователей.

К Определить и протестировать стратегию резервного копирования.

Попробовать дублирование памяти и обработки данных для основных приложений.

#### **Ввод данных**

##### **Сканеры**

У Сканированные образы секретных документов могут оставаться на совместно используемых сканирующих устройствах.

К Завершить сеанс сканирования, выполнив сканирование пустой страницы или несекретного документа. Пользователи должны знать функции ПО сканера. Удалить временные файлы, созданные в процессе сканирования, например, файлы на жестком диске, которые были скопированы с дискеты.

#### **Вывод данных**

##### **Общие положения**

У Устройства вывода данных могут излучать электромагнитные

сигналы, которые можно дистанционно декодировать.

К Запретить парковку автомобилей в зонах рядом с комнатами, в которых используются устройства для вывода секретных данных.

Попробовать эксплуатацию оборудования, проверенного на соответствие стандарту TEMPEST.

Попробовать установить генераторы белого шума, чтобы замаскировать сигналы от оборудования, используемого для вывода секретных материалов.

У Если устройства вывода данных видны из зоны общественного пользования, то информация может оказаться раскрытой.

К Не допускать установки устройств вывода данных там, где неавторизованный персонал / посторонние лица могут прочесть выходные данные.

#### **Разделитель-сортировщик**

У Испорченные бланки документов можно использовать для извлечения финансовой выгоды или как средство передачи секретной информации посторонним лицам.

К Внедрить систему учета бланков секретных документов. Испорченные листы списываются контролирующим лицом и отправляются на измельчение / безопасную утилизацию

У Разделители-сортировщики могут содержать множество движущихся частей, подверженных порче.

К Убедитесь, что разделители-сортировщики подвергаются регулярному обслуживанию.

Установите процедуры для поддержки важнейших приложений каким-либо другим образом, если разделитель-сортировщик ломается.

#### **Упаковщик**

У Упаковочные устройства должны устанавливаться в начале каждого запуска. В связи с этим существует риск, что испорченный бланк документа может быть использован для извлечения финансовой выгоды или передачи информации посторонним лицам.

К Создать систему учета испорченных бланков документов с секретной информацией. Испорченные распечатанные с секретной информацией бланки документов обязательно списываются контролирующим лицом и измельчаются при помощи уничтожителя документов. Запросы на дублирование испорченных распечатанных бланков документов подписываются контролирующим лицом.

### **Лазерный принтер**

У Данные, распечатанные на бумаге при помощи лазерного принтера, могут оказаться стертыми в случае некорректной работы сборки термического закрепления.

К Внедрить регулярные проверки печати данных на бумаге, чтобы обеспечить схватывание тонера на бумаге.

У Лазерные принтеры можно настроить на печать двух копий. Такая настройка нежелательна, если распечатываемая информация является секретной.

К Настроить программное обеспечение на установку количества копий перед печатью каждой страницы.

### **Устройство контактной печати**

У На лентах остаются изображения символов, которые были напечатаны.

К Отправить ленты, использованные для важных приложений, на сжигание.

### **Устройство графического ввода**

У Устройства графического ввода могут давать неправильную информацию в случае износа перьев, их отсутствия или неправильной установки.

К Назначить сотрудников, ответственных за настройку и обслуживание устройств графического вывода. Назначенные сотрудники должны отвечать за контроль качества печати данных.

### **Очереди вывода документов на печать**

У В локальных сетях и в средах микрокомпьютеров задания на печать документов с секретной информацией могут по разным причинам оставаться в очереди вывода документов на печать.

К В случае прерванной или незавершенной печати нужно убедиться, что список очереди вывода документов на печать чист.

### **Дисплей**

У Оставленные без присмотра включенные мониторы могут оказаться источником раскрытия секретной информации неавторизованному персоналу / посторонним лицам.

К Внедрить процедуры переключения экранов мониторов на пустое изображение, если они не используются. Сотрудники должны также блокировать клавиатуру, если оставляют свое рабочее место. Некоторое ПО совмещает функции отключения экрана и блокировки клавиатуры.

### **Фотокопировальное устройство**

#### **Аппаратные средства**

У При помощи фотокопировальных устройств персонал / посторонние лица могут легко выполнить несанкционированное копирование секретной информации.

К Внедрить процедуры, согласно которым копирование распечатанной секретной информации без соответствующего разрешения признается дисциплинарным нарушением.

Ограничить количество и места расположения «временных» копировальных устройств так, чтобы их использование можно было контролировать. Такие устройства не должны быть установлены в зонах, где хранится секретная информация. Они размещаются в зоне, где любой, кто использует копировальное устройство, виден другим сотрудникам.

### **Пишущая машинка**

У На лентах пишущей машинки остается изображение печатного символа.

К Использовать только пишущие машинки, которые разрешены для работы с секретными материалами, и отправлять ленты на утилизацию, которая заключается в их сжигании.

## **Хранение**

### **Бумажные копии документов**

У Бумажные копии документов могут быть уничтожены огнем или повреждены водой.

К Хранить копии важных документов в пожароустойчивых и водонепроницаемых шкафах для хранения документов и/или вне здания.

У Бумажные копии документов можно использовать для удаления секретной информации из узла.

К Регистрировать бумажные копии документов с секретной информацией. Копирование документов с секретной информацией выполняется только санкционированным персоналом в безопасной зоне. Внедрить процедуры, согласно которым несанкционированное копирование документов с секретной информацией признается дисциплинарным нарушением.

### **Съемные магнитные носители**

У Магнитные носители можно использовать для выноса больших объемов данных за пределы организации.

К Использовать магнитные носители с корпоративным логотипом. Внедрить процедуры, по которым все магнитные носители подписываются в и за пределами здания. Обращение и хранение пленок, дискет и съемных жестких дисков должно регулироваться прописанными процедурами, подобными тем, что применяются для бумажных документов. Внедрить процедуры, согласно которым запрещается без разрешения выносить магнитные носители из здания или приносить их в здание. В противном случае, данные действия, совершаемые без разрешения, расцениваются как дисциплинарное нарушение.

У Гибкие диски являются одним из основных носителей,

способствующих переносу вирусов с компьютера на компьютер.

К Проверять все отформатированные магнитные носители на наличие вирусов при поступлении этих носителей в здание.

Проверять особенно тщательно диски, приносимые инженерами и студентами. Все диски, которые проверяются, должны снабжаться маркировкой с корпоративным логотипом и подписью проверяющего с указанием даты.

Внедрить процедуры, согласно которым использование персоналом непроверенных гибких дисков признается дисциплинарным нарушением.

У Использованные гибкие диски все еще содержат информацию, даже если файлы были удалены или диски были отформатированы.

К Если гибкий диск или кассета магнитной ленты используются для хранения секретной информации, необходимо маркировать их соответствующим образом и обращаться с ними как с зарегистрированной бумажной копией документа. Магнитные носители, которые использовались для хранения секретной информации, должны быть размагничены / очищены до их повторного использования. Если магнитный носитель ломается с хранимыми на нем секретными данными, он считается конфиденциальным мусором и уничтожается или сжигается.

#### **Несъемные магнитные носители**

У На жестких дисках могут храниться очень большие объемы информации. Здесь легко можно забыть про секретные файлы.

К При первом использовании жесткого диска для хранения секретной информации жесткий диск обязательно должен быть зарегистрирован. Регистрация такого жесткого диска отменяется только после его проверки на отсутствие секретных файлов сотрудником службы поддержки. Все секретные файлы должны быть безопасно удалены.

У Контроль доступа к микрокомпьютерам осуществляется очень слабо по сравнению с контролем доступа к системе сети. Если жесткие диски микрокомпьютеров используются для хранения секретной информации,



высок риск несанкционированного изменения или раскрытия информации.

К        Блокировать микрокомпьютеры, когда они не используются. Обеспечивать безопасность на месте для ограничения доступа к комнатам с микрокомпьютерами. Установить пакеты контроля доступа и пакеты шифрования данных на компьютерах, которые используются для хранения очень важной информации. Использовать взаимозаменяемые жесткие диски, которые можно удаленно блокировать, если компьютер не используется.

У        Информацию на поврежденных жестких дисках не всегда удается безопасно удалить.

К        В случае отказа жесткого диска с секретной информацией уничтожить диск, если безопасно удалить информацию с него невозможно.

У        Несъемные диски выходят из строя. Если на диске хранятся большие объемы временных данных, их потеря может быть очень серьезной.

К        Резервное копирование больших по объему жестких дисков на гибкие диски отнимает много времени, поэтому персонал неохотно выполняет регулярное резервное копирование данных. Накопители на бегущей магнитной ленте выполняют резервное копирование информации быстро и легко. Установить накопители на бегущей магнитной ленте на компьютеры с большим объемом временной информации на жестких дисках. Ленты / диски для резервного копирования должны храниться для трех копий. По крайней мере, одна резервная копия должна храниться удаленно. Обновление резервных копий выполняется циклически.

Ленты резервных копий должны храниться в безопасном месте и должны быть маркированы с указанием их содержания.

### **Съемные оптические носители**

У        Оптические диски легко спрятать. На них можно хранить очень большие объемы информации.

К        Оптическим дискам с секретной информацией обязательно присваивается серийный номер, на основании которого они регистрируются.

Единственный безопасный способ их утилизации - это сжигание.

У Если поверхность диска поцарапана, возможна частичная или полная потеря данных на оптическом диске.

К Обращаться со всеми оптическими дисками нужно крайне осторожно, чтобы не допустить появления царапин на их поверхности, которые могут повредить отражательное качество диска и «скрыть» основные части данных. В случае повреждения таблицы размещения файлов диска последний становится нечитабельным.

### **Несъемные оптические носители**

У На оптических дисках хранится много информации, и часто информация на дисках не может быть стерта.

К В случае повреждения оптического диска он подлежит уничтожению.

У Большие объемы данных, сохраненных на оптических дисках, могут создать проблемы для резервного копирования.

У Если оптический диск не содержит критически важных данных, которых больше нигде нет, то не нужно дублировать такой диск или создавать его резервную копию. Обычно оптические диски содержат статическую информацию, такую как справочные материалы или программы ПО, которые уже являются дубликатами или резервными копиями существующих данных. Если это не так и информация важна, дубликаты можно получить или сделать на оптических дисках WORM (запоминающее устройство без возможности перезаписи). Также можно копировать на ленту обычным способом. Современные ленточные системы резервного копирования обеспечивают надежное резервное копирование гигабайтов информации. Для удаленного хранения применяются стандартные стратегии резервного копирования.

### **Микрофильм / микрофиша**

У Фильм и микрофишу может легко уничтожить огонь, а также их можно потерять или украсть.

**К**        Никогда не полагаться на одну копию фильма / микрофиши с ключевыми данными. Хранить архивные копии в удаленном месте.

Обращаться с микрофишей / фильмом как с зарегистрированными файлами. Хранить их в безопасном месте; регистрировать дату, время и фамилию и имя создателя при их выпуске.

## **Люди**

### **Персонал**

#### **Угрозы общего характера**

**У**        Среди персонала могут оказаться непорядочные сотрудники и сотрудники, подвергающиеся шантажу.

**К**        При приеме на работу новых сотрудников необходимо сделать обычные запросы проверки их трудового стажа и образования. Персонал, который допускается к работе с важной информацией, необходимо проверить более тщательно, чтобы выяснить наличие у них преступной или социальной деятельности, которая могла бы стать причиной совершения ими мошеннических действий или причиной их шантажа. Обратить особое внимание на финансовое положение, участие в подрывных организациях, семейное положение, психологическое состояние и любые свидетельства наркотической зависимости. Проверки должны повторяться через определенный промежуток времени. Программы информирования по обеспечению безопасности должны обращать внимание на необходимость сотрудников быть бдительными и на положительные преимущества обращения за помощью для себя или других.

**У**        Неправильное разделение обязанностей делает компрометацию любым лицом более разрушительной, может склонить персонал к совершению мошеннических действий и может привести к высоким коэффициентам ошибок при вводе / обновлении данных.

**К**        Убедиться в правильном разделении обязанностей между сотрудниками, отвечающими за авторизацию, ввод данных, прием, платежи

по счетам, хранение финансовых инструментов, аудит; аналитиками систем, программистами, службой контроля внесения изменений, службой контроля предоставления доступа и программистами, отвечающими за информационные библиотеки.

У При недостатке контролируемости персонал, скорее всего, будет больше совершать ошибок или превышать свои полномочия.

К Убедиться, что имеющиеся информационные системы в организации обеспечивают достаточный уровень идентификации, аутентификации и входа в систему для поддерживаемой системы учета и контроля пользователей.

У Недостаток знаний в области последовательности операций и действий в экстренных ситуациях является источником ошибок и причиной неисправностей систем.

К Убедиться, что все сотрудники, работающие с информационными системами, обладают достаточным уровнем знаний о последовательности операций и действий в экстренных ситуациях согласно требованиям их обязанностей и ответственности.

У Сотрудники, занимающие высокие должности, могут поручить авторизацию сделок в компьютеризованной среде подчиненным в случаях, когда они никогда бы такого не сделали в неавтоматизированной системе.

К Настроить соответствующие схемы авторизации для электронных документов. Усовершенствовать общую среду контроля образования и программ, которые повышают осведомленность, участие руководства и контроль.

### **Ключевой персонал**

У Ключевой персонал, который играет важную роль в силу своих обязанностей и особых навыков, может отсутствовать на рабочем месте длительный период времени.

К Предусмотреть альтернативные или резервные кадры, которые

могли бы заменить ключевой персонал в случае необходимости.

### **Ввод данных**

У Данные при вводе можно удалить, неправильно отредактировать или создать. К Программное обеспечение должно включать в себя проверки подтверждения правильности ввода данных для всех ключевых полей, проверки идентификации и аутентификации.

Предусмотреть авторизацию и группирование там, где возможно.

### **Запросы**

У Любой, кто получает право выполнять запросы в пределах системы, может стать источником несанкционированного раскрытия информации.

К Система учета и контроля пользователей и слежение за процессами являются основным средством защиты от несанкционированного раскрытия информации. Дополнительная защита обеспечивается самой информационной системой посредством нанесения на распечатываемые документы соответствующих меток конфиденциальности, тем самым гарантируя, что печать документа выполняется через системный раздел контроля вывода данных на печать, который может регистрировать в журнале любые распечатываемые секретные данные. Сотрудники должны обладать минимальным набором прав доступа согласно занимаемым ими должностям.

Любая неудачная попытка получения доступа в систему должна регистрироваться в журнале и проверяться службой внутреннего аудита. Если 100% проверка не практикуется, то необходимо выбрать статистический образец, чтобы гарантировать, что контроль осуществляется равномерно во времени. Такие проверки проводятся службой внутреннего аудита или командой по аудиту систем.

### **Обращение с распечатанными документами**

У Существует риск копирования распечатанных данных сотрудниками по работе с печатными документами, их потери или передачи

неуполномоченным посторонним лицам.

К Все секретные распечатываемые данные должны передаваться через независимые разделы по работе с выходными данными, причем персонал, работающий с выходными данным, не должен иметь доступа к копировальным устройствам и не должен иметь прав вывода данных на печать. Их единственная роль должна заключаться в регистрации печатных документов с секретной информацией и их передачи лицам, для которых они предназначены.

### **Программисты**

У Программисты могут повредить средства контроля актуальных информационных систем.

К Закрывать доступ для программистов к актуальным информационным системам. За копирование нового программного обеспечения из среды разработки в актуальную систему должна отвечать служба контроля внесения изменений.

У Программисты могут вводить скрытые функции в свои программы, такие как бомба замедленного действия или логическая бомба.

К Программирование должно состоять из унифицированных модулей. Каждый блок (модуль) должен пройти экспертную оценку для предотвращения включения нежелательных функций.

У Программы могут создавать угрозу целостности или доступности информационных систем, если они были недостаточно тщательно протестированы.

К Выполнять тестирование всех программ по блокам, чтобы обеспечить ожидаемые выходные сигналы от ожидаемых входных сигналов. Тестирование должно проводиться сотрудником, независимым от программиста, и официально документироваться как часть процедур контроля качества. Как только блок проходит тестирование, программист больше не имеет к нему доступа.

У Работу программ, для которых плохо составлена документация,

сложно поддерживать, в результате чего может быть нарушена доступность или целостность зависимых информационных систем.

К Документация должна быть включена в процедуры контроля качества. Блок не может пройти контроля внесения изменений, пока оформление на него документов не закончено.

У Доступность информационных систем может подвергаться риску, если инструкции для пользователя не соответствуют программам актуальных информационных систем.

К Заполнение пользовательской документации об изменениях должно быть необходимым условием копирования в актуальную систему нового блока.

### **Аналитики**

У Если аналитиками были допущены ошибки проектирования, то доступность и целостность системы может быть нарушена.

К Проектная документация должна включать спецификации, которые понятны заказчикам. На каждом этапе проектирования проектная документация должна обязательно подписываться заказчиком. Прототипы являются отличным способом подтверждения выполнения требований заказчика до перехода к полному функциональному проектированию.

У Аналитики имеют более широкое представление о взаимодействии информационных систем, чем программисты. В связи с этим существует риск, что они могут воспользоваться своими знаниями, чтобы обойти средства контроля.

К Закрывать аналитикам доступ для записи к исходному коду. Аналитики также не должны иметь доступа к компиляторам или ассемблерам, которые могли бы дать им возможность разработать свои собственные приложения.

Аналитики не должны обладать правом запуска или авторизации конфиденциальных сообщений.

## **Системная поддержка**

У Сотрудники службы поддержки выполняют роль хранителей информации, которая принадлежит другим. В связи с этим существует риск, что они могут внести изменения в информацию или программы или без разрешения распечатывать данные.

К Сотрудники службы поддержки не должны иметь доступа к компиляторам или ассемблерам, которые могли бы дать им возможность разработать свои собственные программы. Они также не должны иметь доступа к исходному коду актуальных информационных систем. Продавцы операционных систем часто предусматривают мощные средства внесения изменений с целью непосредственного изменения программ или данных. Проконсультируйтесь у продавца по поводу возможностей системы, которые можно использовать, чтобы обойти средства контроля системы, и установите для таких средств автономный режим работы. Использование средств изменения системы должно требовать ввода пароля, известного только начальнику по модификациям. Программист, отвечающий за библиотеку носителей, должен регистрировать факты выдачи утилит для служебного пользования. Каждый факт применения утилит для служебного пользования фиксируется в журнале. Сотрудники службы внутреннего/системного аудита должны проверять журналы, которые заполняются супервизором по оперативной деятельности и программистом, отвечающим за библиотеку носителей.

Если блок управления доступом операционной системы достаточно сложен для назначения доступа, копирования и реализации средств контроля для названных утилит, тогда на этот механизм можно положиться в большей степени, чем на автономный режим работы утилит. В случае адаптации данного порядка сотрудники службы внутреннего / системного аудита должны регулярно проверять права доступа и настойчиво требовать от привилегированных пользователей частого изменения своих паролей. Каждый раз, когда используются системные средства внесения изменений,



необходимо менять пароль выполнения.

### **Системные программисты**

У Системные программисты отвечают за поддержание и обслуживание среды операционной системы. Техническая поддержка прежде всего включает операционную систему. Кроме того, в нее могут входить программное обеспечение управления сетью, системы управления базами данных, программное обеспечение обработки операций и программное обеспечение управления хранением данных. Очень часто руководство имеет слабое представление о работе системных программистов, что приводит к плохому контролю их деятельности. Системные программисты могут случайно или намеренно уничтожить всю систему.

К Исключить доступ системных программистов к исходному коду или структурам данных любых актуальных информационных систем. Исключить также доступ системных программистов к компиляторам или ассемблерам в актуальной среде. Разрешить доступ системных программистов посредством программного обеспечения управления доступом к файлам, которые они могут изменять на законных основаниях. Регистрировать в журнале все действия системных программистов.

Исключить доступ системных программистов к программному обеспечению системы контроля доступом или файлам данных.

Все изменения программного обеспечения операционной среды должны осуществляться в среде разработки и проходить экспертную оценку.

В редких случаях, когда экстренные изменения нужно выполнить без официального контроля качества, проверка обязательно проводится после внесения таких изменений.

### **Контроль внесения изменений**

У Служба контроля внесения изменений отвечает за копирование программ и данных из среды разработки в актуальную среду. В связи с этим существует риск, что сотрудники этой службы могут злоупотребить

доступом к актуальной среде, изменив актуальные программы или данные.

К Сотрудники службы контроля внесения изменений не должны иметь доступа к средствам разработки программ, которые предоставили бы им возможность скомпилировать свои собственные программы. Мониторинг действий сотрудников службы контроля внесения изменений должен осуществляться службой внутреннего / системного аудита.

### **Программисты, отвечающие за библиотеку носителей**

У Программисты, отвечающие за библиотеку носителей, осуществляют техническую поддержку и выдачу данных и программ в автономном режиме работы. Если эти программисты имеют доступ к системе, существует риск внесения ими изменений в информацию, которую они контролируют.

К Исключить доступ программистов, отвечающих за библиотеку носителей, к любому программному обеспечению, которое предоставило бы им возможность подделывать содержимое носителей, за которые они отвечают.

### **Логический контроль доступа**

У Служба контроля доступа отвечает за обслуживание профилей пользователей, которые определяют области доступа для каждого конкретного пользователя. В связи с этим, существует риск, что сотрудники службы контроля доступа сами предоставят себе права, которые не соответствуют их функциям.

К Регистрировать в журнале любые изменения профилей доступа. Исключить для сотрудников службы контроля доступа право отключения ведения журнала или изменения его содержимого. Служба внутреннего / системного аудита должна проверять профили доступа, обращая особое внимание на права доступа информированных пользователей и пользователей, которые имеют доступ к особо важным программам / данным.

### **Физический контроль доступа**

У В нерабочие часы охранники в силу своих обязанностей имеют доступ в охраняемые зоны. В связи с этим, существует риск злоупотребления ими такой привилегией.

К Охранники не должны иметь прав доступа к информационным системам. В нерабочие часы вывод секретной информации должен быть заблокирован; на всех компьютерах должен быть выполнен выход из системы, и компьютеры должны быть выключены.

### **Аудиторы**

У Аудиторам требуется расширенный доступ к информационным системам и журналам. В связи с этим, существует опасность, что аудиторы случайно или намеренно нарушат целостность системы.

К Запретить для аудиторов доступ для записи в любых разделах, кроме их собственного. Предоставить аудиторам доступ только для чтения в другие разделы на основании принципа необходимого знания.

### **Владельцы данных**

У Владельцами некоторого объема информации является персонал, который отвечает за обслуживание данной информации. В первую очередь владельцы отвечают за обеспечение безопасности своих собственных данных. В связи с этим, существует риск злоупотребления ими такими привилегиями.

К Между сотрудниками, которые являются владельцами информации, обязанности должны быть распределены таким образом, чтобы гарантировать, что изменение, уничтожение, создание или вывод на печать секретной информации требует участия нескольких человек.

### **Пользователи данных**

У Пользователям данных предоставляются права доступа к информации владельцами данных. В связи с этим, существует риск, что пользователи превысят полномочия, предоставленные им владельцами.

К Предоставлять минимальный объем прав пользователям данных

согласно их правомерной потребности в доступе к информации. Регистрировать в журнале доступ к важной информации и расследовать необычные схемы поведения.

### **Хранители данных**

У Хранители данных отвечают за техническую поддержку инфраструктуры, которая обеспечивает доступ к информации и мерам безопасности, заданным владельцами. В связи с этим, существует риск, что хранители данных могут превысить свои полномочия, случайно или намеренно уничтожив, раскрыв или изменив информацию, которой они располагают.

К Предоставить хранителям минимальный набор прав доступа к информации, которой они располагают. Для обеспечения доступа к информации сотрудникам оперативной службы не нужно ее читать или изменять. Им нужно только знать, что процесс X требует наборов данных A, B и C, которые хранятся на устройстве Q. Нет необходимости и нежелательно для них знать подробности функционирования процессов, которые они обслуживают. Определенным категориям хранителей, таким как системные программисты, администраторы данных и сетевые администраторы, может потребоваться доступ для чтения или записи к актуальным данным. Очень важная информация должна шифроваться так, чтобы она не могла быть раскрыта сотрудникам службы поддержки в ходе мониторинга сети или обслуживания системы. Разумнее всего избегать принятия на работу в операционный отдел сотрудников, которые обладают знаниями в области программирования систем или приложений. Лица, знающие машинный код, представляют особую опасность, поскольку они способны разработать небольшие программы, не используя ассемблер или компилятор. Там, где возможно, сделать невозможным для операционного персонала создавать выполняемые файлы. Это единственная опция, когда операционная система может отличить выполняемый файл от других файлов, а система управления доступом может контролировать возможности

пользователей изменять состояние файлов, которые они создают или изменяют.

### **Подрядчики**

#### **Обслуживание**

У Инженеры по обслуживанию часто обладают глубокими знаниями операционной системы и аппаратного обеспечения. Благодаря этому они могут воспользоваться «лазейками» для нарушения безопасности системы.

К Не оставлять без присмотра работающих инженеров по обслуживанию и не допускать выноса за пределы сети файлов с важной информацией.

У Во многих системах для «пользователей, выполняющих обслуживание системы» установлен пароль по умолчанию. Этот пароль можно использовать для получения несанкционированного доступа к системе.

К Узнать у продавца системы заданных по умолчанию пользователей и их пароли и менять регулярно пароли для данных пользователей и особенно после каждого посещения специалиста по обслуживанию.

### **Консультанты**

У Консультанты неизбежно получают ценную конфиденциальную информацию организации.

К Обязательно требовать от консультантов подписания соглашения о неразглашении конфиденциальной информации. Если им нужен доступ, в частности, к важным системам, они должны пройти «досмотр».

Изменить пароль / данные пользователя, которые известны консультанту, по истечении действия его контракта.

### **Посторонние лица**

#### **Посетители**

У Допуск посетителей в зоны, где работают с конфиденциальной информацией или ее обрабатывают, может привести к нарушению безопасности.

К Обязательным требованием для посетителей является ношение бейджей с фамилией и именем. Персонал должен требовать пропуск у лица, которого он не знает или который не надел бейдж. В охраняемых зонах посетителей нужно сопровождать постоянно.

Держите посетителей подальше от зон, где работают с важной информацией. Если посетителям нужно посмотреть важную информацию, сначала они должны подписать соглашение о неразглашении конфиденциальной информации. Необходимо также убедиться, что они не видели больше, чем нужно.

### **Злоумышленники**

У Злоумышленники могут нарушить конфиденциальность, целостность и доступность информационных систем.

К Многоуровневая система безопасности обеспечивает наилучшую защиту информации. Избегать гласности. Затруднить проникновение в периметр. Установить оборудование обнаружения злоумышленников. Блокировать вход в помещения, которые обеспечивают доступ к важному оборудованию. Использовать систему контроля доступа, чтобы затруднить работу с информационными системами, даже если злоумышленник получил доступ к терминалу.

### **Здания**

#### **Территория организации**

У Есть риск, что помещение организации будет физически повреждено. Отдельные риски, влияющие на вашу территорию, зависят от ваших местных условий.

К Разработать аварийные планы, которые включают план возобновления критически важных функций в случае повреждения или разрушения здания. Аварийные должны ежегодно тестироваться.

У Злоумышленники могут проникнуть на территорию, создав угрозу доступности, целостности или конфиденциальности информационных систем.

К Физическое обеспечение безопасности территории должно соответствовать средней важности информационных систем. Крайне важные приложения можно защитить, обеспечив более высокие уровни безопасности мест, необходимых для осуществления их поддержки. Базовый уровень безопасности территории включает охранников, которые контролируют людей, входящих и выходящих из здания. Окна первого этажа должны быть заперты, когда помещения остаются без присмотра, и оснащены охранными сигнализациями. Общественная парковка не должна находиться в зонах, близких к критически важному оборудованию. Пожарные двери должны открываться наружу и должны быть оборудованы стеклянными болтами и сигнализациями, подключенными к центральной панели управления в офисе службы безопасности.

У Здания, которые используются для поддержки хорошо разрекламированных крайне критических функций, особенно уязвимы.

К Держать в секрете местоположение средств, которые поддерживают критически важные функции. Избегать ненужной огласки. Если планы здания стали известны посторонним лицам, необходимо предпринять более усиленные меры безопасности, чтобы компенсировать повышенные риски.

У Территории, расположенные недалеко от густонаселенных областей, в большей степени подвержены воздействию гражданских беспорядков.

К Территории поддержки основной информационной системы должны быть по возможности расположены вдали от городских агломераций.

У Здания образовательных учреждений особенно уязвимы к грабежам и попыткам проникновения в систему.

**К** В зданиях образовательных учреждений часто физический и логический контроль доступа выполняется слабо. Убедитесь, что охрана помещений, в которых размещено легко транспортируемое имущество/ресурсы, представляющее интерес для злоумышленников, обеспечивается на более высоком уровне по сравнению с базовым уровнем защиты. Средства контроля системы учета пользователей должны в первую очередь использоваться для ключевых систем, доступных из зданий образовательных учреждений.

### **Ключевые помещения**

#### **Ввод / обновление данных**

**У** Зоны, где вводится и обслуживается информация, представляют сосредоточие угроз конфиденциальности и целостности информационных систем.

**К** Зоны ввода данных, по возможности, должны быть недоступны персоналу без обоснованной необходимости такого доступа.

Компьютеры с доступом к средствам для обновления критической информации не должны быть видны из зон общественного пользования. Эти компьютеры нельзя оставлять без присмотра и с выполненным в систему входом.

Приложения, которые обновляют ключевую информацию, должны закрывать сеансы в случае отсутствия активности на клавиатуре в течение нескольких минут. Если информация имеет критическое значение для ключевых информационных систем, приложение должно повторно проводить идентификацию и аутентификацию через определенные промежутки времени и регистрировать в журнале все внесенные изменения. Для особо критической информации следует настроить приложения так, чтобы изменения нельзя было завершить до тех пор, пока они не будут подтверждены разрешающим должностным лицом.

### **Обработка**

**У** Зоны, где выполняется обработка информации, могут



предоставлять широкие возможности разрушения, повреждения информационных систем или получения доступа к ним.

К Разрешить доступ в соответствии с выполненным разделением обязанностей там, где возможно.

У Мейнфреймы часто имеют определенные требования к условиям эксплуатации. Наличие таких требований может привести к естественной изоляции ключевых компьютеров от персонала, который не работает с ними. В связи с тем, что небольшие компьютеры стали более мощными, на них перенесли ключевые приложения. Небольшие компьютеры могут работать в стандартной офисной среде. Использование распределенной обработки данных в некоторых случаях приводит к тому, что информационные системы становятся зависимыми от большого количества территориально рассредоточенных небольших компьютеров. Перенос прикладных систем с больших компьютеров на малые приводит к пренебрежению защитой ключевых компьютеров, делая их уязвимыми при неправильной эксплуатации и при отказе вследствие воздействия окружающей среды.

К Компьютеры с критическими функциями поддержки должны быть физически изолированы от общей офисной среды.

Обеспечить защиту источников питания компьютеров, которые играют существенную роль в критически важных информационных системах.

### **Печать**

У Вывод важной информации на печать должен осуществляться через защищенные зоны таким образом, чтобы его можно было проконтролировать и зафиксировать в журнале. В случае бланков финансовых документов кража распечатанных документов может нанести материальный ущерб организации. В случае задачи сохранения конфиденциальности распечатываемых данных, даже краткий взгляд постороннего человека на распечатываемые данные может привести к потере конфиденциальности.

К Разрешить доступ в помещения, используемые для вывода на

печать ценной или важной информации, только сотрудникам службы по работе с печатной документацией. Физический и логический контроль доступа должен реализовывать разделение обязанностей между сотрудниками, отвечающими за управление и регистрацию напечатанных документов, и сотрудниками, отвечающими за вывод на печать или авторизацию таких документов.

### **Хранение**

У Зоны, где хранится информация, являются привлекательной целью для получения несанкционированного доступа, поскольку здесь накапливается большой объем информации.

К Важная информация должна храниться в защищенных архивах / библиотеках. Разрешить доступ только для программистов-библиотекарей, которые должны проверять наличие разрешения у сотрудников, запрашивающих доступ, на получение данных и регистрировать в журнале выдачу информации.

У Если организация делает только единичные архивные копии информации, возрастает риск потери целостности и доступности информации.

К Адаптировать политику резервного копирования, которая гарантирует, что, по крайней мере, две копии ключевой информации хранятся в территориально рассредоточенных местах. Целостность машиночитаемых архивов должна проверяться регулярно, а архивы на магнитных носителях подлежат копированию, по крайней мере, раз в три года.

### **Запросы**

У Помещения, где обрабатываются запросы, особенно уязвимы к угрозам, нарушающим доступность или целостность информационных систем.

К Продумать аварийные планы, которые позволят персоналу, работающему с запросами, соблюдать критически важные требования в

случае отказа информационных систем или аппаратного оборудования, поддерживающего эти системы.

У Помещения, которые используются как центры по обработке запросов, могут оказаться особенно уязвимыми к угрозам нарушения конфиденциальности информации.

К Процедуры должны определять условия для обеспечения информацией каждой категории и потребности регистрации выдачи информации. Ограничить доступ в зоны, в которых выполняется обработка конфиденциальных запросов. Программное обеспечение должно обеспечивать автоматический выход из системы в случае отсутствия в течении определенного времени активности на клавиатуре. Система учета и контроля пользователей является существенным аспектом контроля запросов. Важно иметь возможность определять действия лиц, а также ограничивать эти действия. Такой контроль может снизить угрозы нарушения конфиденциальности, если оборудование по обработке запросов установлено в разных местах. Например, сделать одну группу персонала ответственной за составление ответов на все запросы от лиц, чьи фамилии начинаются с букв от А до Д, а другие группы, ответственными за другие буквы. Фрагментирование способности получать доступ и упорядочивать информацию может снизить уязвимость к нарушению. Доступ к особенно важной информации должен обеспечиваться через авторизацию от второго оператора / супервизора прежде, чем она будет показана. Компьютеры запросов должны быть размещены таким образом, чтобы их нельзя было увидеть из зон общественного пользования, и чтобы операторы не могли прочесть информацию на экранах других компьютеров.

### **Связь**

У Помещения, в которых размещены распределительные коробки сети, стойки модемов, АТС организации или коробки временных соединений, дают возможность неавторизованному персонала идентифицировать оборудование, связанное с критическими возможностями

и взломать службу или подсоединиться к ней.

**К** Кабеля информационных систем и оборудование связи не должно иметь маркировок, которые хорошо читаются человеком. Предпочтительно использовать зашифрованные метки кабелей. Расшифровка системы кодирования кабелей должна храниться дистанционно и под замком. Маркировка кабелей должна быть сделана таким образом, чтобы затруднить опознавание маршрута, составленного ключевыми соединениями.

Распределительные коробки, стойки модемов и телефонные АТС должны быть защищены. Доступ должен быть разрешен только для обслуживающего персонала и сетевых администраторов.

### **Операции актуальных прикладных систем**

**У** Доступ к компьютерам, которые работают с актуальными приложениями, может облегчить обход мер, предназначенных обеспечивать целостность, доступность и конфиденциальности систем.

**К** Доступ в помещения, где размещены компьютеры, являющиеся ключевыми компонентами актуальных информационных систем, должен быть разрешен только для операционного персонала. Распределение обязанностей гарантирует, что операционный персонал не сможет создавать входные сообщения, проектировать или разрабатывать программы или получать доступ к выводу на печать важной информации, заданного системами, с которыми работает операционный персонал. Гарантия недоступности к выводимым на печать данным легко реализуется, если защищенный вывод данных возможен только на устройства, находящиеся за пределами операционной зоны, а операционному персоналу вход туда запрещен.

### **Разработка приложений**

**У** Прикладное программное обеспечение потенциально является самым мощным средством, подвергающим опасности целостность информационных систем. Программисты или другие специалисты, имеющие

доступ к среде разработки, могут выполнить скрытые действия в системе в обход средствам контроля.

**К** Поручать работу программистам на модульной основе. Каждый модуль должен иметь входные и выходные спецификации. Экспертная оценка и тестирование блока должны обеспечить защиту системы от внедрения скрытых функциональных возможностей. Сотрудники службы контроля внесения изменений должны быть отделены от программистов приложений как физически, так и на уровне управления.

Доступ в помещения, где осуществляется разработка приложений защищенных систем, должен быть разрешен только для программистов. Доступ для аналитиков и сотрудников службы контроля внесения изменений запрещен.

Жесткие меры обеспечения контроля системой учета пользователей и использование системы контроля последней версии должны гарантировать постоянную регистрацию осуществляемых в системе действий; лиц, которыми эти действия осуществляются, и дату выполнения этих действий. В нерабочие часы средства разработки должны быть недоступны.

### **Функции систем**

**У** Средства диагностики и управления системами можно использовать для перехвата сетевого трафика и обхода средств контроля.

**К** Ограничить доступ к определенным терминалам и средствам контроля отчетности, используемым для контроля использования, тем же образом, что и для программистов приложений. Разрешить физический доступ к терминалам системы только для сотрудников службы поддержки систем, которые должны работать парами.

### **Электроэнергетическая установка**

**У** Электропитание является основным источником энергии для информационных систем. Прекращение подачи электропитания может вызвать уничтожение информации и, в случае скачков напряжения, вывести из строя аппаратные средства, которые обеспечивают работу системы.

**К** Все ресурсы/имущество информационных систем должны сглаживать работу источников электропитания, обладающих функциями устранения вредных скачков напряжения в питании. Ключевое машинное оборудование, такое как файловые серверы, требуют наличия бесперебойного блока питания, чтобы гарантировать, что оборудование, по крайней мере, завершит работу должным образом в случае прекращения подачи энергии.

Доступ в помещения с электроэнергетическими установками должен быть разрешен только для обслуживающего персонала.

#### **Бланки для документов**

**У** Наличие незаполненных бланков необходимо для непрерывной работы некоторых систем. Примером таких бланков могут быть лицензии и сертификаты. Уничтожение запасов вызовет остановку в обслуживании.

**К** Резервные запасы важных бланков должны храниться в любом удаленном здании, где выполняется обработка данных, и в альтернативном месте в пределах главного здания. Резервные запасы должны храниться при том же уровне безопасности, что и основной запас. Кладовщик должен регулярно проверять комплектность / пригодность к использованию резервных запасов.

#### **Приготовление пищи / курение**

**У** Приготовление пищи и курение являются основными источниками пожара, который приводит к отказу информационной системы.

**К** Запретить курение и приготовление пищи в зонах рядом с ключевыми ресурсами/имуществом. Помещения, где разрешено готовить пищу или курить, должны быть оборудованы противопожарными системами. В частности, в помещениях, предназначенных для курения, должны быть установлены огнестойкие пепельницы и мусорные ведра.

#### **Ценные бланки для документов**

**У** Бланки документов, которые можно использовать для извлечения материальной выгоды или в качестве основания получения прав,

такие как бланки пропусков, подлежащие оплате заказы или чеки, являются ценным объектом для кражи.

**К** Критически важные бланки для документов должны быть снабжены серийными номерами и должны храниться в запертом хранилище. Работник(и) склада обязан(ы) вести учет выдачи бланков, включая любые бракованные бланки. Стараться обеспечить проведение сверки документации, которая может объяснить ее использование по признакам разрешенных к выдаче бланков и бракованных бланков. Помещения, где хранятся ценные бланки документов, должны охраняться, а доступ в них должен быть разрешен только для уполномоченных подотчетных сотрудников.

### **Документация**

#### **Программное обеспечение**

**У** Ведение документации важно для программного обеспечения, подлежащего обслуживанию. В связи с этим, существует риск потери, уничтожения или кражи документации. Сильная мотивация к совершению кражи возникает там, где программное обеспечение выполняет функции, которые представляют коммерческую ценность или раскрывают информацию, являющуюся собственностью фирмы, или секретную информацию.

**У** Проверка документации должна быть включена в процедуры контроля качества. Как только документация утверждена, зарегистрированные копии должны быть занесены в реестр сотрудниками службы контроля внесения изменений.

Резервные копии документации актуальной системы должны храниться в другом здании.

С документацией зависимых систем необходимо обращаться также, как с зарегистрированным файлом. Копии должны нумероваться; копирование запрещается, а а выдача должна осуществляться по принципу служебной необходимости. Когда копии не используются, их следует хранить в

запертом удаленном месте.

### **Аппаратные средства**

У Ресурсы/имущество информационных систем часто представляют интерес получения выгоды, легко транспортируются и их можно легко повредить.

К Полная опись всех материальных ресурсов/имущества информационных систем должна храниться, поддерживаться и проверяться в организации.

У Руководства по аппаратным средствам требуются редко, но их необходимо хранить на случай, когда они понадобятся. Их часто трудно заменить, и они могут содержать информацию, которой может воспользоваться человек, намеревающийся вторгнуться в систему.

К Хранить руководства к аппаратным средствам в запертых библиотеках или в пределах охраняемых зон. Регистрировать выдачу руководств особенно в случаях, когда получено разрешение на вынос руководства из помещения, в котором размещено оборудование. Хранить копии важных руководств к аппаратным средствам в другом здании.

### **Процедуры**

У Рабочие руководства дают сотрудникам важную информацию, а также могут дать посторонним лицам представление о том, как работают системы, что нежелательно.

К Руководства с описанием процедур должны выдаваться названным лицам, регистрироваться и храниться в секрете. Руководства по процедурам должны выдаваться указанным лицам, регистрироваться и охраняться. Все руководства должны помечаться грифом секретности на каждой странице, а в важнейших руководствах должны быть указания на каждой странице, поясняющие, что копирование не разрешено. Храниться копии руководств по процедурам за пределами своей территории.

### **Аварийный план**

У По своей природе аварийные планы требуются не часто и в



моменты, когда организация находится в стрессовом состоянии. Есть риск, что они устареют или будут недоступны в момент возникновения чрезвычайной ситуации. Кроме того, их может использовать кто-нибудь, кто хочет прекратить обслуживание.

**К** Аварийные планы проверяются и испытываются с регулярными интервалами, в большинстве ситуаций каждый год, но чаще, если доступность крайне важна. Копии соответствующих разделов должны храниться в безопасности в резервных помещениях.

### **Планы этажей**

**У** Планы этажей являются очень полезными документами для потенциального нарушителя.

**К** Храните архитектурные чертежи далеко в запертом помещении. Это особенно важно, если чертежи содержат функциональную информацию.

### **Схемы кабельных соединений**

**У** Схемы кабельных соединений нужны для обслуживания систем, подключенных к сети. Потеря этих схем значительно затрудняет обслуживание информационных систем или диагностику отказов сети. Схемы также очень полезны для тех, кто заинтересован в проникновении или прерывании работы информационных услуг, предоставляемых сетью.

**К** Схемы сети должны составляться и обновляться в любом случае при внедрении новой маршрутизации или соединения.

Копии схем кабельных соединений должны храниться в зданиях резервного хранилища, чтобы облегчить восстановление системы в случае повреждения главного здания.

Доступ к схемам кабельных соединений должен быть разрешен только для персонала, отвечающего за управление кабельными соединениями / администрирование сети.

### **Словарь данных**

**У** Словарь данных содержит указатель по структуре всех постоянных информационных систем. Он является важным инструментом

для разработки новых информационных систем. Он может оказаться бесценной информацией для желающих проникнуть в информационные системы данной организации. К Внедрить поддержку словаря данных и процедуры контроля внесения изменений, которые гарантируют, что словарь отражает текущую структуру данных в имеющихся информационных системах организации. Хранить копии в удаленных местах.

Поддерживать ведение журнала копий документов, которые получены из словаря данных, и обращаться с конфиденциальными выписками как с зарегистрированными файлами.

### **Условия эксплуатации**

#### **Кондиционирование воздуха**

У Большие компьютеры и их периферийные устройства часто предполагают строгие требования к среде. Несоответствия условиям среды, указанным производителем, могут привести к отказу машин и спорам по поводу технического обслуживания.

К Настроить программу регулярного технического обслуживания для важного оборудования кондиционирования воздуха.

Попробовать установить запасное оборудование для кондиционирования воздуха в помещениях, где могут выйти из строя ключевые ресурсы.

#### **Электропитание**

У Неблагоприятное воздействие на ресурсы/имущество информационных систем может оказать уменьшение или

увеличение напряжения или частоты источников электроэнергии. К

Все компьютеры должны быть защищены источниками питания с ограничителем перенапряжения. Ключевые ресурсы должны быть защищены источниками бесперебойного питания.

#### **Вода**

У Для некоторых мейнфреймов требуется подача охлажденной воды. Сбои в подаче воды могут привести к серьезным повреждениям

компьютера.

**К** Обеспечить постоянную подачу воды под контролем операционного персонала, а не персонала по обслуживанию здания. Сотрудники по обслуживанию нередко случайно отключают подачу холодной воды на время выходных / периоды отсутствия активной деятельности. Рассмотрите резервную подачу холодной воды или автоматическое, нормальное, выключение соответствующих компьютеров в случае сбоя в водоснабжении.

### **Освещение**

**У** Темнота может сильно подорвать планы по работе в чрезвычайных ситуациях.

**К** Предусмотреть резервное освещение.

### **Отходы**

#### **Бумага**

**У** При работе информационных систем часто накапливается огромное количество использованной бумаги. Она может стать источником утечки информации из организации.

**К** Все распечатанные документы должны быть в соответствии с правилами отмечены грифом секретности. Рассмотрите возможность уничтожения материала особой важности посредством измельчения. Мешки с пометкой «конфиденциальный мусор» должны использоваться для материала, ожидающего сжигания. В организациях часто пренебрегают обеспечением безопасности в отношении отходов. Мешок с отходами, содержащий материал, который мог бы быть помещен в зарегистрированную папку, должен соответствовать такому же уровню безопасности, который был бы применен к папке.

### **Магнитные носители**

**У** Магнитные носители содержат фрагменты файлов, которые копировались на них, даже после удаления таких файлов с носителей.

**К** Ненужные магнитные носители должны быть почищены,

размагничены или уничтожены с соблюдением мер безопасности.

### **Оптические носители**

У Как правило, эффективно стереть информацию с оптических носителей невозможно.

К Лучшим способом уничтожения ненужных использованных оптических средств хранения информации является их сжигание.

### **Бланки для документов**

У Ненужные бланки финансовых документов можно использовать в незаконных целях.

К Устарелые бланки финансовых документов должны официально списываться и утилизироваться как конфиденциальные отходы.

Убедиться, что материалы бухгалтерского учета учитывают утилизацию предварительно пронумерованных бланков для документов.

## **Приложение I**

### **Определения**

#### **Классификация информации:**

Информация без пометок: информация, не помеченная или не классифицированная иным способом, для которой достаточно принятия мер безопасности стандартных эффективных систем управления. Информация, которая доступна общественности. Например: отчеты за определенные периоды деятельности организации, режим работы персонала, руководства и публикации, управление общим имуществом, публикуемые уставы, вакансии, мнения и т.д.

Помеченная информация: информация, обозначенная как нуждающаяся в защите, кроме информации государственной важности.

Классифицированная информация: информация государственной важности.

#### **Информационная система / приложение:**

«Приложение специального программного обеспечения для выполнения конкретной работы. Любой набор шагов, соблюдаемый при осуществлении финансовой, административной или программной деятельности», например, информационная система кредиторов.

В операционной среде микрокомпьютера приложения могут быть очень простыми, такими как текстовый редактор создания отчета WordPerfect для работы с клавиатуры, настройки формата и печати, или комплексными, как программа СААТ для загрузки данных клиента, выборки образцов, анализа результатов и печати образцов или результатов.

Используемое программное обеспечение, например, программы СААТ, Lotus или WP, не нужно путать с применением программного обеспечения, выборочной ревизии или годового отчета. Обычно название приложения представляет собой комбинацию наименования используемого программного обеспечения и разработанного приложения, как например,

Аудиторская выборка СААТ, Финансовый анализ Lotus, Аудиторский отчет WP.

В целях оценки безопасности похожие приложения можно относить в одну группу.

«Логический» контроль доступа и отчетность как часть системы безопасности

«Логический» контроль доступа, использующий имена и пароли, обеспечивает ограничение доступа к данным для каждого конкретного пользователя. Такой доступ обеспечивается посредством системы безопасности, которая определяет, к чему пользователь имеет доступ и какие действия он может осуществлять, и поддерживает функции поддерживает функции отчетности путем создания контрольного журнала, в котором регистрируется работа пользователя с компьютером.

Контроль доступа, как и любой другой контроль, не считается эффективным и надежным, если он не соответствует поставленным задачам и не может быть отслежен. Контрольный журнал служит свидетельством того, что мера по контролю доступа работает, как предполагается, и дает средство исследования неисправностей и определения областей, в которых контроль можно усовершенствовать. В системе безопасности компьютера, контрольный журнал представляет собой архивный файл, созданный и сохраняемый системой через контроль паролей и шифровки. Использование контрольного журнала прозрачно для пользователя. При многих системах безопасности, администратор по безопасности имеет доступ к архивным файлам контрольных журналов всех пользователей. Отдельные пользователи имеют доступ для чтения к своим собственным контрольным журналам.

### **Принцип служебной необходимости**

Основополагающий принцип политики безопасности – ограничить доступ к данным и ресурсам для людей, которым нужен такой доступ, что включает определение требований к предоставлению данных и ресурсов. В

компьютерной среде это включает физический и (или) логический контроль доступа к данным и ресурсам (система безопасности). Например, в контрольно-ревизионном управлении пользователи защищают информацию о клиенте, аудите и административных вопросах, чтобы не дать посторонним случайно прочесть, изменить или уничтожить информацию.

### **Уязвимость информации:**

Доступность: качество или состояние информации, служб, систем и программ оказываться своевременно доступными («на уровне организации»).

Конфиденциальность: качество или состояние информации, выраженное в степени ее важности («в случае раскрытия данной информации организация понесет убытки»).

Целостность: качество или состояние информации быть точной и полной («в случае изменения, неточности или неполноты информации организация может понести убытки»).

### **Оценка уровня риска нарушения безопасности**

Оценка уровня риска нарушения безопасности представляет собой результат объединения оценки последствий для деятельности и оценки вероятности/риска возникновения угрозы. Оценка риска нарушения безопасности может быть:

Высокая: очень серьезные последствия - обоснованная вероятность. События с высокой вероятностью проявления и настолько серьезными последствиями для деятельности, что разумно предпринять профилактические и восстановительные шаги. Уровень ожидаемых повреждений настолько высок, что не составляет труда сделать точные прогнозы вероятности проявления.

Средняя: значительные последствия - неизвестная вероятность. Последствия для деятельности таковы, что необходимо предпринять определенные шаги. Обзор угроз и их вероятности необходим для снижения угроз на управляемом уровне.

Низкая: незначительные последствия - любая вероятность. Категория «ну и что». Если данное событие произойдет, оно не причинит значительно вреда. Если кажется, что возможность повреждений низка, то значит, существуют приемлемые угрозы. Необходимость в проведении детального анализа вероятности отсутствует.

### **Инфраструктура безопасности**

Обычно во многих государственных организациях под одинаковыми или разными названиями управление безопасностью поручается:

**Начальнику службы безопасности:** руководителю высшего звена, который отвечает в целом за безопасность в организации. Он является связующим звеном для всех других государственных учреждений и полностью несет ответственность за все вопросы безопасности в пределах своей собственной организации.

**Директору по безопасности:** старшему управляющему с переданными начальником службы безопасности полномочиями, который несет ежедневную ответственность за управление по всем вопросам безопасности в пределах организации.

**Сотруднику, отвечающему за компьютерную безопасность:** старшему управляющему с переданными полномочиями от начальника службы безопасности и отчитывающемуся перед директором по безопасности, который несет ежедневную ответственность за управление по вопросам безопасности компьютеров и технологий в пределах организации.

**Команде по обеспечению безопасности:** команде сотрудников, сформированной из насколько возможно широкого поперечного среза организации. Команда нуждается в полной поддержке и заинтересованности высшего руководства, необходимых для выполнения проверки безопасности и получения признания ее результатов. Например, желательно, чтобы представитель пользователей был влиятельным членом пользовательского сообщества и лидером в команде. Пользователи и высшее руководство охотнее примут рекомендации по безопасности от команды, поскольку



обычно они подозрительно относятся к отчетам, составленным «техническими специалистами».

Корпоративная политика безопасности, утвержденная высшим руководством, реализуется для поддержки стратегии информационных систем, которая основана на миссии и целях, определенных в заявлении о корпоративной политике.

Обычно Руководящий комитет по информационным системам под председательством руководителя высшего звена играет важную роль в гарантии того, что все информационные системы в организации разработаны и используются в соответствии с корпоративными целями и стратегиями. Руководящий комитет по информационным системам контролирует внедрение политики информационных систем и политики безопасности.

### **Принципы управления безопасностью**

Защита безопасности должна соответствовать уязвимости защищаемых данных;

Защита безопасности должна всегда оставаться с информацией, когда информация передается или обрабатывается; а также

Защита безопасности должна быть постоянной во всех ситуациях.

Эти принципы внедряются, определяя важность данных с точки зрения целостности, конфиденциальности и доступности и применение конкретных элементов схемы безопасности, которая включает людей, физические объекты, опыт и процедуры, аппаратные средства, программное обеспечение, приложения и элементы защиты для резервного копирования.

# **Методика проверки обеспечения безопасности информационных систем**

## **Руководство по проверке обеспечения безопасности информационных систем в государственных организациях**

### **Том 3: Метод детализации обеспечения безопасности информационных систем**

#### **Неавтоматизированный количественный подход к обеспечению безопасности информационных систем<sup>9</sup>**

---

<sup>9</sup> Утверждено из методологии, разработанной Национальным контрольно-ревизионным управлением Великобритании. Настоящий документ направлен только на предоставление общего описания подробного и количественного метода анализа риска, используемого различными способами большинством коммерческих пакетов анализа риска. Настоятельно рекомендуется, чтобы использовалось программное обеспечение для микрокомпьютера с этим подробным методом анализа риска.

## **1. Обзор**

1.1 Программа безопасности информационных систем предназначена для снижения риска потери конфиденциальности, целостности и доступности этой информации до приемлемого уровня.

1.2 Метод обеспечения безопасности информационных систем предназначен для облегчения создания всеобъемлющей, экономически эффективной программы обеспечения безопасности, охватывающей все основные информационные системы. Данный метод должен помочь пользователям создать уровень безопасности, соответствующий их требованиям. Поиск подходящего уровня безопасности включает анализ рисков и управление рисками.

1.3 Анализ рисков используется для определения степени, в которой информационные системы подвергаются рискам. Он влечет за собой оценку угроз для информационных систем, оценку частоты, с какой эти угрозы возникают, и оценку последствий для организации в случае возникновения угроз. «Риск нарушения» рассчитывается путем объединения оценки последствий и посчитанной частоты угроз.

1.4 Управление рисками включает выбор наименьших по стоимости контрмер, которые снижают опасность для организации до приемлемого уровня. Контрмеры представляют собой шаги, которые предпринимает организация для снижения частоты угроз или для снижения последствий в случае возникновения угроз.

1.5 Определение ценности является ключевым элементом установления приемлемого уровня безопасности, а пользователи являются ключевым элементом для определения ценности. Из этого следует, что на раннем этапе необходимо определить группы пользователей. Оценку каждой системы можно выполнить по ее пользователям. Система без пользователей или система, в которой пользователи не придают значения получаемой информации, не имеет ценности и не нуждается в обеспечении, не говоря уже о защите.

1.6 Если системам ничего не угрожает, то обеспечивать их безопасность не требуется. Настоящий метод должен помочь в идентификации угроз в отношении конфиденциальности, целостности или доступности информационных систем. Он предусматривает определение всех компонентов, которые должны присутствовать, чтобы пользователи продолжали получать надежное обслуживание, и последующее рассмотрение событий, которые могут негативно повлиять на каждый из компонентов. Метод также предусматривает определение способов, при помощи которых может произойти утечка информации из каждого компонента информационной системы.

1.7 После определения ценности системы и угроз, которые ей характерны, можно сформулировать требования к безопасности. Требования к безопасности представляют собой перечень мер, которые необходимо предпринять для снижения рисков, с которыми сталкиваются пользователи, до приемлемого уровня. За реализацию этих мер и их поддержку отвечает персонал инфраструктуры безопасности.

1.8 Метод обеспечения безопасности информационных систем состоит из следующих этапов:

- (1) Определить политику безопасности.
- (2) Создать инфраструктуру безопасности.
- (3) Идентифицировать информационные системы.
- (4) Идентифицировать угрозы / слабые места
- (5) Выполнить оценку ценности/важности систем.
- (6) Оценить требования к безопасности для каждой системы.
- (7) Внедрить и поддерживать программу обеспечения безопасности и процедуры, соответствующие политике безопасности.

## **2. Инфраструктура**

2.1 Политика безопасности должна отражать стратегию информационных систем, которая сама должна основываться на миссии и целях, определенных в заявлении о корпоративной политике. Начинать разработку стратегии безопасности информационных систем, пока не определена корпоративная стратегия или стратегия информационных

систем, не следует. Совет директоров должен продумать политику безопасности. Политика должна быть одобрена главой организации. Обязательно назначается сотрудник службы безопасности (SO), который контролирует внедрение политики безопасности.

2.2 Если в организации имеется или планируется иметь расширенные информационные системы, необходимо основать Руководящий комитет по информационным системам (ISSC). Председателем Руководящего комитета по информационным системам должен быть член совета директоров. Роль Руководящего комитета по информационным системам заключается в обеспечении разработки стратегии информационных систем в соответствии с корпоративными целями и постоянном обновлении стратегии безопасности. Необходимо назначить начальника по безопасности информационных систем (ISSO) и рассмотреть вопрос о создании службы безопасности информационных систем (ISSG). Безопасность информационных систем является сферой деятельности. Роль службы безопасности заключается в осуществлении деятельности как центра разработки безопасности информационных систем.

2.3 Отчет о политике безопасности должен установить рамки для программ безопасности, касающихся каждой крупной информационной системы. Крупные организации часто выпускают рекомендации по обеспечению безопасности, которые устанавливают стандарты безопасности с подробным описанием. Рекомендации помогают персоналу перевести требования политики безопасности в программу безопасности собственных систем.

2.4 Рабочие процедуры по безопасности (SOP) разрабатываются в форме руководств, в которых указаны подробности о процедурах, необходимых для поддержки программы по безопасности. SOP особенно важны, так как многие меры безопасности неэффективны, если сотрудники не понимают и не соблюдают соответствующих процедур.

2.5 Программы обучения и информирования сотрудников являются

важной частью инфраструктуры безопасности. Необходимо включить обучение по безопасности в комплекс мер при принятии на работу и продолжать его вместе с курсами повышения квалификации с регулярными интервалами. Использование плакатов, брошюр и руководств может способствовать дальнейшему укреплению основных элементов программы безопасности.

### **3. Границы**

3.1 Первый этап проверки обеспечения безопасности информационных систем заключается в установлении границ проверяемой системы. Эту задачу можно выполнить путем идентификации сообщества пользователей.

3.2 В случае малого взаимодействия между информационными системами можно без труда установить пользователей выходных данных системы. В высоко интегрированных системах искусственная граница должна быть согласована для того, чтобы выполнить проверку в разумном масштабе.

3.3 Очень важно обеспечить заинтересованность высшего руководства в проверке и, в особенности, согласование им границ такой проверки.

3.4 Идеально начать с полной информационной модели организации, в которой должна проводиться проверка. Эта модель должна показывать поток информации как в пределах организации, так и между организацией и другими учреждениями за ее пределами. Модель может работать как основа для программы обеспечения безопасности информационных систем, которая будет охватывать все ключевые системы при завершении проверки.

### **4 Служба безопасности**

4.1 Первое проявление заинтересованности высшего руководства в обеспечении безопасности информационной системы должно заключаться в создании Службы безопасности информационной системы (ISSG). Служба

безопасности должна отвечать за выполнение политики по безопасности, разработанной высшим руководством, и за определение изменений, которые необходимо внести в связи с нововведениями в информационные системы организации, или угрожающих факторов, которые перед ними стоят.

4.2 Если результаты проверки должны быть приняты по всей организации, важно обеспечить, чтобы служба безопасности состояла из как можно более широкой представительной выборки организации. Особенно это важно, если проверка проводится сторонним консультантом.

4.3 Группа по внутреннему аудиту должна создать глубокое понимание информационных систем в организации и должна будет сыграть важную роль при обеспечении эффективного выполнения рекомендаций по безопасности. Служба безопасности может использовать рабочие документы по внутреннему аудиту для лучшего понимания информационных систем в организации, но маловероятно, что члены секции внутреннего аудита захотят играть здесь активную роль, так как это поставит под угрозу их независимость на стадии проверки.

4.4 Основную роль в объяснении того, как работает система, и в оценке информации, полученной из системы, должны играть пользователи информационной системы. Сотрудничество пользователей важно для успешного выполнения программы обеспечения информационной безопасности. Пользователи с большей вероятностью примут рекомендации по безопасности, если членом группы будет влиятельный представитель сообщества пользователей. Представитель пользователей часто становится хорошим руководителем группы, так как это дает гарантии и высшему руководству, и пользователям, часто с подозрением относящимся к отчетам, составляемым «техническими специалистами».

4.5 Если система сильно компьютеризирована, тогда в службу нужно включить аналитика систем, чтобы в случае необходимости он помог объяснить работу компьютерной системы и посоветовать понятный и

целесообразный способ документирования потоков информации.

4.6 Если структура системы проста, то специалисты по компьютерной безопасности могут не потребоваться. Но в случае с комплексными компьютеризированными системами их помощь требуется как при оценке угроз в отношении систем, так и при формулировке контрмер.

## **5. Угрозы / уязвимость**

5.1 Первый этап оценки угроз по отношению к системе состоит в определении цепочки средств, которые участвуют в предоставлении информации каждому крупному пользователю. Помните о целях информационной безопасности – конфиденциальность, сохранность и доступность – и обдумайте все элементы в системе, в которых любой из этих элементов может быть поставлен под угрозу. Перечень ресурсов/имущества для сетевого приложения включает больше пунктов, чем для не автоматизированного или автономного приложения. Автономная программа обработки текстов будет уязвима через экран, принтер, клавиатуру и через любое устройство хранения, такое как гибкие диски, бумага или пленки. Подключенная к сети система может быть уязвимой во многих других местах, включая компьютеры, принтеры, телекоммуникационное оборудование, подключенное к сети, сетевые кабели, а также центральные и локальные диски.

5.2 Создайте форму по каждому ресурсу или группе ресурсов, которые вы определили, и затем составьте список всех событий, которые могут поставить под угрозу сохранность, доступность или конфиденциальность информационных систем, подключенных к ресурсу. Для каждого события нужно сделать оценку его вероятности возникновения в пределах года. Это может оказаться сложным, если такое событие не случалось в истории работы ваших информационных систем. Статистика страхования в страховых компаниях может помочь вам сделать реалистичную оценку частоты возникновения редкого события. При любом подходе существует элемент неопределенности. Записи о прошлом опыте



связаны только с обнаруженными событиями; тогда как безопасность системы может быть нарушена, но не обнаружена. Кроме того, не существует гарантии, что события будут происходить с той же частотой, что и в прошлом.

5.3 Оценка предполагаемой частоты возникновения событий, которые могут нарушить безопасность ваших информационных систем, играет важную роль в обосновании затрат на меры по защите системы. Если вы не заинтересуете высшее руководство своей стратегией, которую адаптируете для оценки частоты возникновения событий, то маловероятно, что высшее руководство обратит внимание на ваши рекомендации.

5.4 Если уже предприняты меры для снижения вероятности того, что работа информационной системы будет скомпрометирована, необходимо принять к сведению эти меры и выполнить оценку годовой стоимости поддержания этих мер, а также эффект, который они оказывают на частоту возникновения событий, негативно влияющих на работу информационных систем. Эту информацию можно использовать позже для принятия решения относительно необходимости замены существующих мер более эффективными.

## **6. Оценка**

6.1 Результатом анализа угроз и слабых мест системы является перечень событий, которые могут негативно повлиять на работу информационной системы. Вы должны согласовать предполагаемую частоту возникновения каждого события. Следующий этап заключается в обсуждении с пользователями последствий каждого события.

6.2 Оценки, которые дают пользователи в отношении последствий каждой угрозы, будут использованы в качестве одного из обоснований затрат на принятие мер безопасности. Важно представить последствия в денежном выражении и оценить их на основе единообразных принципов. Многие последствия, которые могут появиться в связи с нарушением информационной системы, не имеют непосредственных финансовых

последствий. В таких случаях необходимо разработать шкалы, которые можно использовать для представления нефинансовых последствий в денежном выражении.

6.3 Ключевая шкала составляется для финансовых потерь и может иметь следующий вид:

Потери <sup>10</sup>	Степень
£10 млн. +	10
£4 млн. - £10 млн.	9
£2 млн. - £4 млн.	8
£1 млн. - £2 млн.	7
£500 000 - £1 млн.	6
£250 000-£500 000	5
£100 000-£250 000	4
£50 000-£100 000	3
£10 000-£50 000	2
£1 000-£10 000	1

6.4 Другая используемая шкала может касаться безопасности персонала:

Результат	Степень
Гибель 100+ людей	10
Гибель 50+ людей	9
Гибель 25+ людей	8
Гибель 10+ людей	7
Гибель 5+ людей	6
Гибель 1-5 человек	5
Гибель 1 человека	4
Потеря зрения или 2+ конечностей	3
Потеря конечности или слуха	2
Минимальный вред	1

6.5 Шкалы выше приведены в качестве примеров. Можно разработать много других шкал, таких как юридическая ответственность, политические препятствия и организационное разрушение. Шкалы, которые вы разрабатываете, должны быть согласованы друг с другом и охватывать все основные последствия в случае потери информационных систем.

6.6 Как только шкалы утверждены высшим руководством, вы можете перейти к проведению опроса пользователей информационных

---

<sup>10</sup> В настоящем документе символ фунтов стерлингов (£) используется условно, и вместо него можно использовать любую национальную валюту. Возможно потребуются адаптировать пределы шкал к валюте страны и согласованным уровням важности.

систем. Необходимо попросить их взвесить последствия каждого события, установленного в ходе анализа угроз / слабых мест. Пользователи могут идентифицировать последствия по нескольким шкалам. Будьте осторожны, избегайте двойного подсчета. Если уничтожение информации может привести к потере жизни, и это может привести к судебному процессу, убытки от которого в размере 100 000 фунтов будут компенсированы и будет только 5 000 других убытков, то вы можете отнести этот риск к 4 степени по шкале личной безопасности, что может быть признано как среднее значение 175 000 фунтов на шкале финансового ущерба. Прибавление к этой цифре других расходов 5 000 фунтов приведет к общим убыткам с финансовой точки зрения 180 000 фунтов, что соответствует общему уровню 4 по шкале финансового ущерба.

6.7 После проведения опроса ключевых пользователей системы в вашем распоряжении окажется серия оценок. Если последствия, указанные пользователями, покажутся необоснованными, то оценки должны быть скорректированы высшим руководством. Затем составив перечень всех последствий, указанных пользователями для каждого события, можно определить оценку события.

## **7. Требования к безопасности**

7.1 Требования к безопасности представляют собой заявление о том, сколько стоит потратить на обеспечение защиты каждого ресурса/имущества в системе. Такая оценка основана на оценках важности и частоты каждого неблагоприятного события. Оценки пользователей должны быть переведены в денежное выражение по средним точкам финансовой шкалы. Частота возникновения события указывается количеством раз проявления предполагаемого события в каком-либо году. Это значение будет меньше единицы, если событие происходит редко. Соберите вместе все последствия, указанные пользователями для каждого события, и исключите любые повторения. Если вы затем прибавите финансовые значения и умножите на частотность случая, это даст Ожидаемые годовые убытки (ALE) для одного

конкретного события, влияющего на один конкретный ресурс.

7.2 Вычисление ALE нужно повторять для каждого события, которое может существенно негативно сказаться на каждом ресурсе, связанном с каждой из проверяемых информационных систем. Когда эта работа будет завершена, ресурсы можно сортировать по ALE. Сортированный список должен сформировать основу для плана действий по разработке программы безопасности.

## **8. Контрмеры**

8.1 Требование безопасности подчеркивает ресурсы, представляющие значительный риск конфиденциальности, сохранности или доступности проверяемых информационных систем. Контрмеры – это шаги, предпринимаемые для снижения частотности угрожающих ресурсам информационных систем факторов или воздействия в случае возникновения угрожающих факторов.

8.2 Следует начинать с установления мер противодействия для защиты ресурсов с наибольшим ALE. Продумайте шаги, которые могли бы снизить частоту или последствия событий, имеющих самые серьезные последствия. Выясните затраты на них, включая обучение, обслуживание и сбои, которые они могут вызвать. После оценки мер, которые можно ввести, рассмотрите сокращение ALE, которого они, как ожидается, могут достигнуть.

8.3 Разовая контрмера, такая как введение охранника на входе в помещение, может сократить ALE, связанные со многими событиями, влияющими на многие ресурсы. Вам понадобится убедиться, что в случае введения каждой меры отражены все выгоды от нее. Для каждой меры противодействия ведите список воздействия событий / ресурсов, ALE которых от них зависят, а также величину ожидаемой перемены.

После определения контрмер, которые бы снизили наибольшие ALE до уровня следующего по величине значения ALE, необходимо направить свое внимание на следующее событие /ресурс в списке.

8.5 Каждый раз при выборе контрмеры вам придется согласовывать ALE любых других событий / ресурсов, на которые повлияет мера противодействия. По мере передвижения вниз по списку, оставшиеся ALE будут меньше. Нужно остановиться, когда оставшиеся значения ALE становятся ниже порогового значения, которое, по вашему мнению, примет руководство.

8.6 В рекомендациях руководству нужно отражать те меры противодействия, которые приносят наибольшее снижение ALE при наименьших расходах. Руководство может решить принять риск любого события, влияющего на любой ресурс в информационной системе, но оно должно осуществлять это исключительно в свете анализа ALE, чтобы знать о величине рисков, которые они принимают. Если руководство решает не вводить контрмеру, то вам понадобится переформировать список значений ALE с использованием списка воздействия для контрмеры.

## **9. Управление безопасностью**

9.1 Как только перечень контрмер согласован, их необходимо внести в программы безопасности и операционные процедуры безопасности. Группа по безопасности информационной системы должна отвечать за проведение выбранных контрмер.

9.2 Служба внутреннего аудита должна проверить рабочие документы по оценке рисков и управлению рисками и проконтролировать внедрение и эффективность выбранных контрмер.

9.3 Программы и процедуры безопасности требуют обновления с учетом изменений в среде безопасности и информационных системах. Служба безопасности информационных систем должна быть в курсе разработок по обеспечению безопасности информационных систем и информирована обо всех значимых разработках в информационных системах организации. Службой должна постоянно отслеживаться потребность в обновлении программы безопасности.

## **Краткий глоссарий**

### **Терминология в области рисков нарушения безопасности<sup>11</sup>**

**Контрмера (К):** Контроль, предназначенный для повышения безопасности путем снижения угрозы, последствий, обнаружения нарушений безопасности или восстановления деятельности после инцидента с нарушением безопасности.

**Синонимы:** Защитное мероприятие, мера безопасности.

**Воздействие:** негативный эффект или последствие проявившейся угрозы.

**Вероятность:** вероятность проявления конкретной угрозы.

**Риск / нарушение:** мера вероятности и размеры последствий конкретной угрозы в информационной системе. Это функция проявления угрозы и возможного убытка как ее результата.

**Оценка рисков:** официальный процесс оценки вероятности используемых слабых мест исходя из эффективности существующих или предложенных мер по обеспечению безопасности.

**Угроза (У):** любое потенциальное событие или действие, которое нежелательно и может повлиять на информационную систему, например, пожар, стихийное бедствие, несанкционированный доступ и т.д.

**Уязвимость:** мера вероятности того, что тот или иной ресурс станет подвергнется воздействию определенного угрожающего фактора.

---

<sup>11</sup> Терминология в области рисков нарушения безопасности может сильно различаться в разных школах. Также, в зависимости от используемой методики, последствия и слабые места можно оценить по наличию существующих мер безопасности или отсутствию каких-либо мер.