

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Кафедра информационной безопасности

Составители
Е. В. Прокопенко
И. В. Чичерин

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Методические материалы

Рекомендованы учебно-методической комиссией специальности 10.05.03
Информационная безопасность автоматизированных систем в качестве
электронного издания для использования в образовательном процессе

Кемерово 2018

Рецензенты

Стенин Д. В. – кандидат технических наук, доцент директор ИИТМА

Сыркин И. С. – кандидат технических наук, доцент кафедры информационных и автоматизированных производственных систем

Прокопенко Евгения Викторовна
Чичерин Иван Владимирович

Управление информационной безопасностью: методические материалы [Электронный ресурс] для обучающихся специальности 10.05.03 Информационная безопасность автоматизированных систем очной формы обучения / сост. Е. В. Прокопенко, И. В. Чичерин; КузГТУ. – Электрон. издан. – Кемерово, 2018.

© КузГТУ, 2018

© Е. В. Прокопенко,
И. В. Чичерин,
составление, 2018

1. Базовые понятия и подходы к управлению информационной безопасностью.

Основные понятия информационной безопасности

Прежде чем говорить об обеспечении безопасности персональных данных, необходимо определить, что же такое информационная безопасность.

Термин «информационная безопасность» может иметь различный смысл и трактовку в зависимости от контекста. В данном курсе под информационной безопасностью мы будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

ГОСТ «Защита информации. Основные термины и определения» вводит понятие информационной безопасности как состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

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

Целостность – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;

Доступность – состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.

Угрозы информационной безопасности – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Атакой называется попытка реализации угрозы, а тот, кто предпринимает такую попытку, – злоумышленником.

Потенциальные злоумышленники называются источниками угрозы.

Угроза является следствием наличия уязвимых мест или уязвимостей в информационной системе. Уязвимости могут возникать по разным причинам, например, в результате непреднамеренных ошибок программистов при написании программ.

Угрозы можно классифицировать по нескольким критериям:

по свойствам информации (доступность, целостность, конфиденциальность), против которых угрозы направлены в первую очередь; по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);

по способу осуществления (случайные/преднамеренные, действия природного/техногенного характера);

по расположению источника угроз (внутри/вне рассматриваемой ИС).

Обеспечение информационной безопасности является сложной задачей, для решения которой требуется комплексный подход. Выделяют следующие уровни защиты информации:

законодательный – законы, нормативные акты и прочие документы РФ и международного сообщества;

административный – комплекс мер, предпринимаемых локально руководством организации;

процедурный уровень – меры безопасности, реализуемые людьми;

программно-технический уровень – непосредственно средства защиты информации.

Законодательный уровень является основой для построения системы защиты информации, так как дает базовые понятия предметной области и определяет меру наказания для потенциальных злоумышленников. Этот уровень играет координирующую и направляющую роли и помогает поддерживать в обществе негативное (и карательное) отношение к людям, нарушающим информационную безопасность.

ФЗ «Об информации, информационных технологиях и о защите информации»

В российском законодательстве базовым законом в области защиты информации является ФЗ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года номер 149-ФЗ. Поэтому основные понятия и решения, закрепленные в законе, требуют пристального рассмотрения.

Закон регулирует отношения, возникающие при:

- осуществлении права на поиск, получение, передачу, производство и распространение информации;
- применении информационных технологий;
- обеспечении защиты информации.

Закон дает основные определения в области защиты информации. Приведем некоторые из них:

- **информация** – сведения (сообщения, данные) независимо от формы их представления;
- **информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
- **информационная система** – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
- **обладатель информации** – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
- **оператор информационной системы** – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.
- **конфиденциальность информации** – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

В статье 4 Закона сформулированы принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации:

1. свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
2. установление ограничений доступа к информации только федеральными законами;
3. открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;
4. равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;
5. обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;
6. достоверность информации и своевременность ее предоставления;
7. неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
8. недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Вся информация делится на **общедоступную** и **ограниченного доступа**. К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. В законе, определяется информация, к которой нельзя ограничить доступ, например, информация об окружающей среде или деятельности государственных органов. Оговаривается также, что ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

Закон выделяет 4 категории информации в зависимости от порядка ее предоставления или распространения:

- 1) информацию, свободно распространяемую;
- 2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
- 3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Закон устанавливает равнозначность электронного сообщения, подписанного электронной цифровой подписью или иным аналогом собственноручной подписи, и документа, подписанного собственноручно.

Дается следующее определение защите информации – представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации.

Таким образом, ФЗ «Об информации, информационных технологиях и о защите информации» создает правовую основу информационного обмена в РФ и определяет права и обязанности его субъектов.

Управление информационной безопасностью (Information Security Management или ISM) – процесс, который обеспечивает *конфиденциальность, целостность* и доступность активов, информации, данных и услуг организации. *Управление информационной безопасностью* обычно является частью Организационного подхода к *Управлению безопасностью*, который имеет более широкую область охвата, чем поставщик услуг, и включает обработку бумажных документов, *доступ* в здания, телефонные звонки и т. п., для всей организации.

Основной целью *ISM* является обеспечение эффективного управления информационной безопасностью всех услуг и деятельности в рамках *Управления услуг*. *Информационная безопасность* предназначена для защиты от нарушения конфиденциальности, доступности и целостности информации, информационных систем и коммуникаций.

1. **Конфиденциальность** – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.

2. **Целостность** - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;

3. **Доступность** - состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.

Цель обеспечения информационной безопасности достигнута, если:

1. Информация доступна тогда, когда это требуется, а информационные системы устойчивы к атакам, могут избегать их или быстро восстанавливаться.

2. Информация доступна только тем, кто имеет соответствующие права.

3. Информация корректна, полна и защищена от неавторизованных изменений.

4. Обмен информацией с партнерами и другими организациями надежно защищен.

Бизнес определяет, что и как должно быть защищено. При этом для эффективности и целостности обеспечения информационной безопасности необходимо рассматривать бизнес процессы от начала до конца, так как слабое *место* может сделать уязвимой всю систему.

Процесс *ISM* должен включать в себя:

- формирование, управление, распространение и соблюдение Политики информационной безопасности и других вспомогательных политик, которые имеют отношение к информационной безопасности. **Политика информационной безопасности (Security Policy)** – политика, определяющая подход организации к управлению информационной безопасностью.

- понимание согласованных текущих и будущих требований бизнеса к безопасности;

- использование *контролей безопасности* для выполнения Политики информационной безопасности и управления рисками, связанными с доступом к информации, системам и услугам. Термин "*контроль безопасности*" является заимствованным из английского языка и в данном контексте означает набор контролер и мер предосторожности, применяемых для аннулирования, уменьшения рисков и противостояния им. То есть *контроль безопасности* состоит из проактивных и реактивных действий;

- документирование перечня *контролей безопасности*, действий по их эксплуатации и управлению, а также всех связанных с ними рисков;

- управление поставщиками и контрактами, требующими доступа к системам и услугам. Осуществляется при взаимодействии с процессом Управления поставщиками;

- контроль всех «брешей» безопасности и инцидентов, связанных с системами и услугами;

- проактивное улучшение *контролей безопасности* и уменьшение рисков нарушения информационной безопасности;

- интеграция аспектов информационной безопасности во все процессы Управления услуг.

Политика информационной безопасности должна включать в себя следующее:

- реализация аспектов Политики информационной безопасности;
- возможные злоупотребления аспектами Политики информационной безопасности;
- политика контроля доступа;
- *политика использования* паролей;
- политика электронной почты;
- политика интернета;
- политика антивирусной защиты;
- политика классификации информации;
- политика классификации документов;
- политика удаленного доступа;
- политика доступа поставщиков к услугам, информации и компонентам;
- политика размещения активов.

Перечисленные политики должны быть доступны пользователям и заказчикам, которые в свою *очередь* обязаны письменно подтвердить свое согласие с ними.

Политики утверждаются руководством бизнеса и ИТ и пересматриваются в зависимости от обстоятельств.

Чтобы обеспечивать информационную *безопасность* и управлять ею, необходимо поддерживать Систему управления информационной безопасностью. **Система управления информационной безопасностью (Information Security Management System или ISMS)** - система политик, процессов, стандартов, руководящих документов и средств, которые обеспечивают организации достижение целей управления информационной безопасностью.



Представлены 5 элементов структуры ISMS:

1. Контроль. Цели контроля:
 - формирование системы управления информационной безопасностью в рамках организации;

- формирование организационной структуры для подготовки, утверждения и реализации Политики информационной безопасности;

- распределение ответственностей;

- формирование документации по контролю.

2. Планирование. Цель планирования – разработать и рекомендовать подходящие метрики и способы измерения информационной безопасности. В первую очередь планирование должно учитывать требования и особенности конкретной организации. Источниками информации для формирования требований к информационной безопасности являются бизнес, риски, планы, стратегия, соглашения (в первую очередь OLA и SLA). При этом важно учитывать моральную, законодательную и этическую ответственности в контексте информационной безопасности.

3. Реализация. Цель реализации – обеспечение подходящих процедур, инструментов и *контролей безопасности* для поддержки Политики информационной безопасности.

В рамках реализации проводятся следующие мероприятия:

- *идентификация активов* – совместно с Управлением конфигурациями;

- классификация информации – информация и информационные хранилища должны быть классифицированы в соответствии с их чувствительностью и значимостью по отношению к трем аспектам информационной безопасности (конфиденциальности, целостности, доступности).

4. Оценка. Цель оценки в рамках ISMS:

- проверка соответствия политики информационной безопасности требованиям к информационной безопасности из SLA и OLA;

- проведение регулярных проверок технической составляющей информационной безопасности для IT систем;

- предоставление информации для регуляторов и внешних аудиторов при необходимости;

5. Поддержка. Цели поддержки ISMS:

- улучшение соглашений в отношении информационной безопасности, например, SLA и OLA

- совершенствование средств и контролей информационной безопасности[10].

Ключевые деятельности в рамках *ISM*:

1) формирование, пересмотр и корректирование Политики информационной безопасности и набора поддерживающих ее вспомогательных политик;

2) реализация и соблюдение политик информационной безопасности, а также обеспечение взаимодействия между ними;

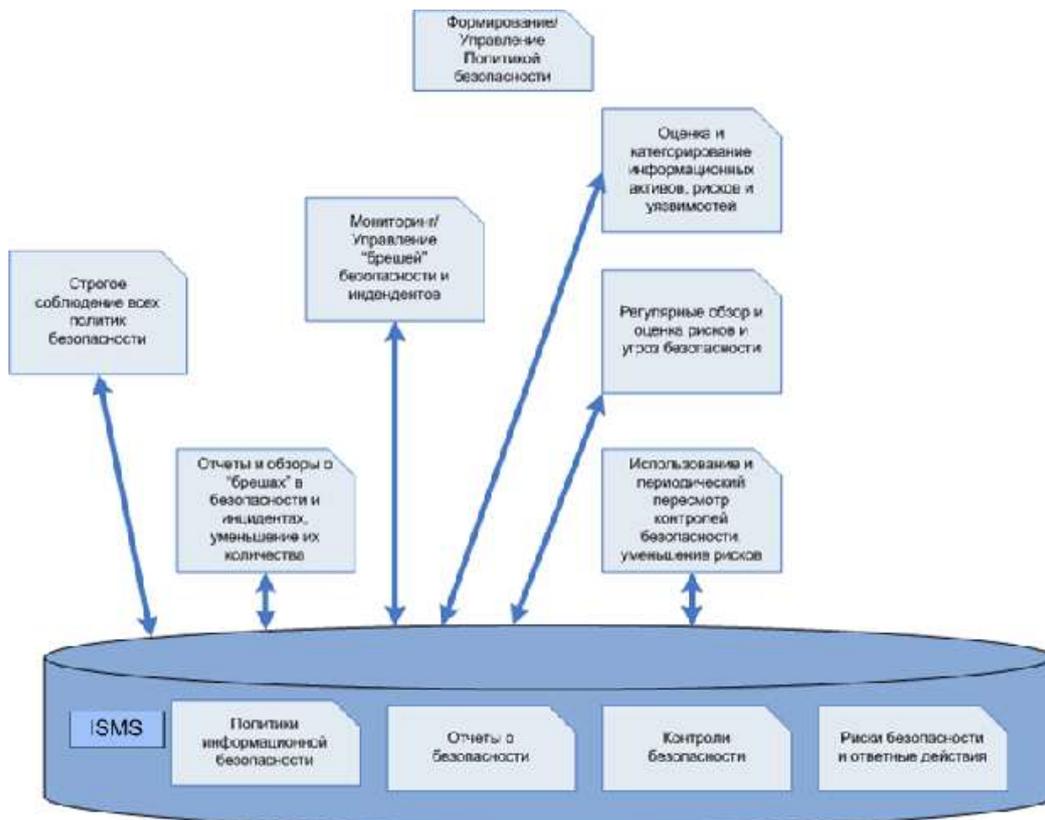
3) оценка и классификация всех информационных активов и документов;

4) использование, пересмотр и корректирование набора *контролей безопасности*, мер по оценке рисков и ответных действий;

5) мониторинг и управление «брешами» безопасности и инцидентами;

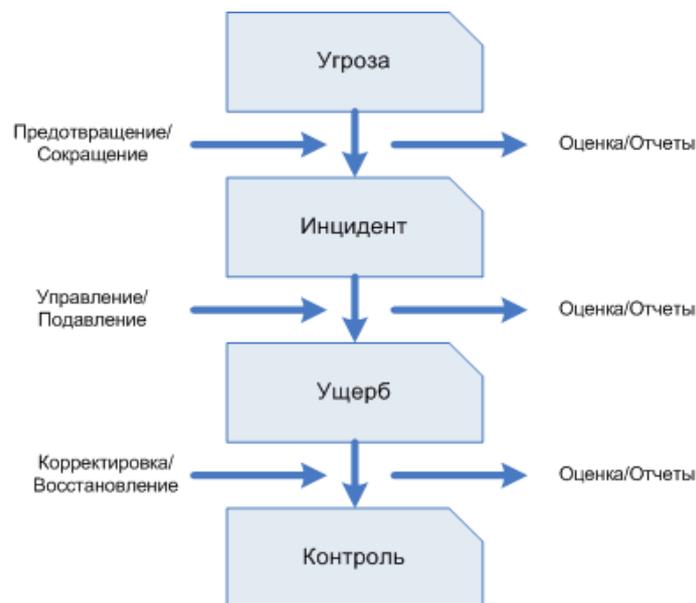
6) анализ, ведение отчетности и уменьшение влияния «брешей» в безопасности и инцидентов;

7) составление расписания и проведение аудитов, тестирования и обзоров.



Ключевые деятельности в рамках ISM

Для обеспечения и поддержки Политики информационной безопасности необходимо сформировать и использовать набор *контролей безопасности*. Для предотвращения инцидентов и правильного реагирования в случае их возникновения используют меры безопасности.



Контроли безопасности

Выделено четыре стадии. Первая стадия – возникновение угрозы. Угрозой является все, что может негативно повлиять на *бизнес-процесс* или прерывать его.

Инцидент – это реализованная угроза. Инцидент является отправной точкой для применения *контролей безопасности*. В результате инцидента появляется *ущерб*. Для управления или устранения рисков также применяются контроли безопасности. Для каждой стадии необходимо подобрать подходящие меры обеспечения информационной безопасности:

- 1) превентивные – меры безопасности, которые предотвращают появление инцидента информационной безопасности. Например, распределение прав доступа.
- 2) восстановительные – меры безопасности, направленные на уменьшение потенциального ущерба в случае инцидента. Например, резервное копирование.
- 3) обнаруживающие – меры безопасности, направленные на обнаружение инцидентов. Например, антивирусная защита или система обнаружения вторжений.
- 4) подавляющие – меры безопасности, которые противодействуют попыткам реализации угрозы, то есть инцидентам. Например, банкомат забирает у клиента карту после определенного количества неправильных вводов PIN-кода.
- 5) корректирующие – меры безопасности, направленные на восстановления после инцидента. Например, восстановление резервных копий, откат на предыдущее рабочее состояние и т. п.

Входами процесса *ISM* являются:

- 1) информация от бизнеса – стратегии, планы, бюджет бизнеса, а также его текущие и будущие требования;
- 2) политики безопасности бизнеса, планы безопасности, Анализ рисков;
- 3) информация от ИТ – стратегия, планы и бюджет ИТ;
- 4) информация об услугах – информация от *SLM*, в частности Портфеля услуг и Каталога услуг, *SLA/SLR*;
- 5) отчеты процессов и анализа рисков от *ISM*, Управления доступностью и Управления непрерывностью услуг;
- 6) детальная информация обо всех инцидентах информационной безопасности и «брешах» в ней;
- 7) информация об изменениях – информация от процесса Управления изменениями, в частности расписание изменений и их влияние на планы, политики и контроли информационной безопасности;
- 8) информация о взаимоотношениях бизнеса с услугами, вспомогательными услугами и технологиями;
- 9) информация о доступе партнеров и поставщиков к услугам и системам, предоставляемая процессами Управления поставщиками и Управления доступностью.

Выходами *ISM* являются:

- 1) всеобъемлющая политика информационной безопасности и другие вспомогательные политики, которые имеют отношение к информационной безопасности;
- 2) система управления информационной безопасностью (*ISMS*), которая содержит всю информацию, необходимую для обеспечения *ISM*;
- 3) результаты переоценки рисков и ревизии отчетов;
- 4) набор *контролей безопасности*, описание их эксплуатации и управления, а также всех связанных с ними рисков;

- 5) аудиты информационной безопасности и отчеты;
- 6) расписание тестирования планов информационной безопасности;
- 7) классификация информационных активов;
- 8) отчеты о существующих «брешах» в информационной безопасности и инцидентах;
- 9) политики, процессы и процедуры для управления доступом поставщиков и партнеров к услугам и системам.

В качестве ключевых показателей производительности процесса Управления информационной безопасностью можно использовать множество метрик, например:

1. защищенность бизнеса от нарушений информационной безопасности
 - процентное уменьшение сообщений о «брешах» в Сервис-деск;
 - процентное уменьшение негативного влияния на бизнес со стороны «брешей» и инцидентов;
 - процентное увеличение пунктов, касающихся информационной безопасности, в SLA.
2. формирование четкой и согласованной политики информационной безопасности, учитывающей потребности бизнеса, то есть уменьшение количества несовпадений между процессами *ISM* и процессами и политиками информационной безопасности бизнеса.
3. процедуры по обеспечению безопасности, которые оправданы, согласованы и утверждены руководством организации:
 - увеличение согласованности и пригодности процедур обеспечения безопасности;
 - увеличение поддержки со стороны руководства
4. механизмы улучшения:
 - количество предложенных улучшений в отношении контролей и процедур;
 - уменьшение количества несовпадений, обнаруженных в процессе тестирования и аудита.
5. информационная безопасность является неотъемлемой частью услуг и процессов *ITSM*, то есть увеличение количества услуг и процессов, в которых предусмотрены меры безопасности [10].

ISM сталкивается со множеством трудностей и рисков на пути обеспечения информационной безопасности. К сожалению, на практике достаточно часто бизнес считает, что вопросами информационной безопасности должна заниматься только ИТ. Еще хуже, когда бизнес не понимает, зачем вообще нужно уделять внимание информационной безопасности. Создание эффективной системы защиты информации влечет за собой большие *затраты*, которые должны быть понятны руководству, так как именно оно принимает решение о финансировании. При этом важно соблюдать баланс – обеспечение информационной безопасности не должно стоять больше самой защищаемой информации.

2. Международные и российские стандарты по УИБ.

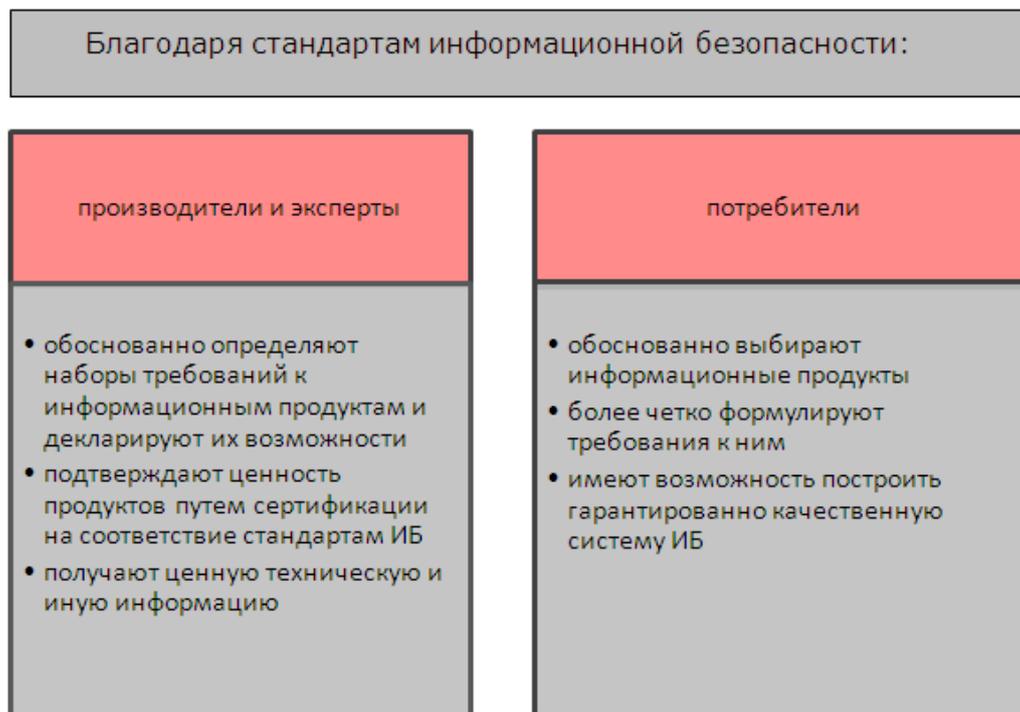
В настоящее время в России наряду с отечественной нормативной базой широко используются около 140 международных стандартов в области информационных технологий. Из них около 30 затрагивают вопросы защиты информации. Некоторые международные стандарты по защите информации приняты и введены в действие в России, но эти стандарты не составляют целостной основы для решения проблем информационной безопасности, особенно в части нормативного регулирования, методического и инструментального обеспечения разработки, оценки и сертификации безопасности ИТ с учетом современного уровня развития, масштабов и многообразия угроз.

Стандарты информационной безопасности – это обязательные или рекомендуемые к выполнению документы, в которых определены подходы к оценке уровня ИБ и установлены требования к безопасным информационным системам.

Стандарты в области информационной безопасности выполняют следующие важнейшие функции:

- выработка понятийного аппарата и терминологии в области информационной безопасности
- формирование шкалы измерений уровня информационной безопасности
- согласованная оценка продуктов, обеспечивающих информационную безопасность
- повышение технической и информационной совместимости продуктов, обеспечивающих ИБ
- накопление сведений о лучших практиках обеспечения информационной безопасности и их предоставление различным группам заинтересованной аудитории – производителям средств ИБ, экспертам, ИТ-директорам, администраторам и пользователям информационных систем
- функция нормотворчества – придание некоторым стандартам юридической силы и установление требования их обязательного выполнения.

Благодаря стандартам информационной безопасности:



Преимущества использования стандартов ИБ разными группами ИТ-сообщества

Согласно Федеральному закону №184-ФЗ «О техническом регулировании», целями стандартизации являются:

– повышение уровня безопасности жизни и здоровья граждан, имущества физических и юридических лиц, государственного и муниципального имущества, объектов с учетом риска возникновения чрезвычайных ситуаций природного и техногенного характера, повышение уровня экологической безопасности, безопасности жизни и здоровья животных и растений;

– обеспечение конкурентоспособности и качества продукции (работ, услуг), единства измерений, рационального использования ресурсов, – взаимозаменяемости технических средств (машин и оборудования, их составных частей, комплектующих изделий и материалов), технической и информационной совместимости, сопоставимости результатов исследований (испытаний) и измерений, технических и экономико-статистических данных, проведения анализа характеристик продукции (работ, услуг), исполнения государственных заказов, добровольного подтверждения соответствия продукции (работ, услуг);

– содействие соблюдению требований технических регламентов;

– создание систем классификации и кодирования технико-экономической и социальной информации, систем каталогизации продукции (работ, услуг), систем обеспечения качества продукции (работ, услуг), систем поиска и передачи данных, содействие проведению работ по унификации.

Основными областями стандартизации информационной безопасности являются:

- аудит информационной безопасности
- модели информационной безопасности

- методы и механизмы обеспечения информационной безопасности
- криптография
- безопасность межсетевых взаимодействий
- управление информационной безопасностью.

Стандарты информационной безопасности имеют несколько классификаций:



Различные классификации стандартов информационной безопасности

Существуют российские стандарты информационной безопасности (ГОСТ Р ИСО/МЭК 15408, ГОСТ Р 51275 и др.), причем Федеральный закон №184-ФЗ «О техническом регулировании» декларирует принцип «применения международного стандарта как основы разработки национального стандарта, за исключением случаев, если такое применение признано невозможным вследствие несоответствия требований международных стандартов климатическим и географическим особенностям Российской Федерации, техническим и (или) технологическим особенностям или по иным основаниям, либо Российская Федерация в соответствии с установленными процедурами выступала против принятия международного стандарта или отдельного его положения».

Необходимость следования некоторым стандартам информационной безопасности закреплена законодательно. Однако и добровольное выполнение стандартов очень полезно и эффективно, поскольку в них описаны наиболее качественные и опробованные методики и решения.

Международные стандарты

- BS 7799-1:2005 – Британский стандарт BS 7799 первая часть. BS 7799 Part 1 – Code of Practice for Information Security Management (Практические правила управления информационной безопасностью) описывает 127 механизмов контроля, необходимых для построения *системы управления информационной безопасностью (СУИБ)* организации, определённых на основе лучших примеров мирового опыта (best practices) в данной области. Этот документ служит практическим руководством по созданию СУИБ

- BS 7799-2:2005 – Британский стандарт BS 7799 вторая часть стандарта. BS 7799 Part 2 – Information Security management – specification for information security management systems (Спецификация системы управления информационной безопасностью) определяет спецификацию СУИБ. Вторая часть стандарта используется в качестве критериев при проведении официальной процедуры сертификации СУИБ организации.

- BS 7799-3:2006 – Британский стандарт BS 7799 третья часть стандарта. Новый стандарт в области управления рисками информационной безопасности

- ISO/IEC 17799:2005 – «Информационные технологии – Технологии безопасности – Практические правила менеджмента информационной безопасности». Международный стандарт, базирующийся на BS 7799-1:2005.

- ISO/IEC 27000 – Словарь и определения.

- ISO/IEC 27001 – «Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования». Международный стандарт, базирующийся на BS 7799-2:2005.

- ISO/IEC 27002 – Сейчас: ISO/IEC 17799:2005. «Информационные технологии – Технологии безопасности – Практические правила менеджмента информационной безопасности». Дата выхода – 2007 год.

- ISO/IEC 27005 – Сейчас: BS 7799-3:2006 – Руководство по менеджменту рисков ИБ.

- German Information Security Agency. IT Baseline Protection Manual – Standard security safeguards (Руководство по базовому уровню защиты информационных технологий).

Государственные (национальные) стандарты РФ

- ГОСТ Р 50922-2006 – Защита информации. Основные термины и определения.

- Р 50.1.053-2005 – Информационные технологии. Основные термины и определения в области технической защиты информации.

- ГОСТ Р 51188-98 – Защита информации. Испытание программных средств на наличие компьютерных вирусов. Типовое руководство.

- ГОСТ Р 51275-2006 – Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

- ГОСТ Р ИСО/МЭК 15408-1-2008 – Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
- ГОСТ Р ИСО/МЭК 15408-2-2008 – Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.
- ГОСТ Р ИСО/МЭК 15408-3-2008 – Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.
- ГОСТ Р ИСО/МЭК 15408 – «Общие критерии оценки безопасности информационных технологий» – стандарт, определяющий инструменты и методику оценки безопасности информационных продуктов и систем; он содержит перечень требований, по которым можно сравнивать результаты независимых оценок безопасности – благодаря чему потребитель принимает решение о безопасности продуктов. Сфера приложения «Общих критериев» – защита информации от несанкционированного доступа, модификации или утечки, и другие способы защиты, реализуемые аппаратными и программными средствами.
- ГОСТ Р ИСО/МЭК 17799 – «Информационные технологии. Практические правила управления информационной безопасностью». Прямое применение международного стандарта с дополнением – ISO/IEC 17799:2005.
- ГОСТ Р ИСО/МЭК 27001 – «Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования». Прямое применение международного стандарта – ISO/IEC 27001:2005.
- ГОСТ Р 51898-2002 – Аспекты безопасности. Правила включения в стандарты.

3. Политика ИБ организации

Политикой информационной безопасности (ИБ) называется комплекс мер, правил и принципов, которыми в своей повседневной практике руководствуются сотрудники предприятия/организации в целях защиты информационных ресурсов.

За время, прошедшее с возникновения самого понятия ИБ, наработано немало подобных политик – в каждой компании руководство само решает, каким образом и какую именно информацию защищать (помимо тех случаев, на которые распространяются официальные требования законодательства Российской Федерации). Политики обычно формализуются: разрабатывается соответствующий регламент. Такой документ сотрудники предприятия обязаны соблюдать. Хотя не все из этих документов в итоге становятся эффективными. Ниже мы рассмотрим все составляющие политики информационной безопасности и определим основные аспекты, которые необходимы для ее эффективности.

Для чего нужна формализация защиты информации

Положения о политике информационной безопасности чаще всего в виде отдельного документа появляются во исполнение требования регулятора – организации, регламентирующей правила работы юридических лиц в той или иной

отрасли. Если положения об информационной безопасности нет, то не исключены определенные репрессии в отношении нарушителя, которые могут вылиться даже в приостановку деятельности последнего.

Также политика безопасности является обязательной составляющей определенных стандартов (местных или международных). Необходимо соответствие конкретным требованиям, которые обычно выдвигают внешние аудиторы, изучающие деятельность организации. Отсутствие политики безопасности порождает отрицательные отклики, а подобные оценки негативно влияют на такие показатели, как рейтинг, уровень надежности, инвестиционная привлекательность и т. д.

Материалы об информационной безопасности появляются на свет, когда высший менеджмент сам приходит к пониманию необходимости структурированного подхода к теме защиты информации. Такие решения могут быть воплощены в жизнь после внедрения технических средств, когда появляется осознание того, что данными средствами надо управлять, они должны быть под постоянным контролем. Зачастую ИБ включает в себя и проблематику взаимоотношений с персоналом (сотрудник может рассматриваться не только как лицо, подлежащее защите, но и как объект, от которого информация должна быть защищена), иные аспекты и факторы, выходящие за рамки исключительно защиты компьютерной сети и предотвращения несанкционированного доступа к ней.

Наличие соответствующих положений говорит о состоятельности организации в вопросах информационной безопасности, ее зрелости. Четкая формулировка правил обеспечения информационной безопасности является свидетельством того, что в данном процессе достигнут существенный прогресс.

Несостоявшиеся политики

Одно лишь наличие документа с названием «Положение об информационной безопасности» не является залогом информационной безопасности как таковой. Если он рассматривается лишь в контексте соответствия каким-то требованиям, но без применения на практике эффект будет нулевым.

Неэффективная политика безопасности, как показывает практика, встречается двух видов: грамотно сформулированная, но не реализуемая, и реализуемая, но внятно не сформулированная.

Первая, как правило, достаточно распространена в организациях, в которых ответственный за защиту информации просто скачивает аналогичные документы из Интернета, вносит минимальные правки и выносит общие правила на утверждение руководства. На первый взгляд, такой подход кажется прагматичным. Принципы безопасности в разных организациях, даже если направленность их деятельности разнится, зачастую похожи. Но проблемы с защитой информации могут возникнуть при переходе от общей концепции информационной безопасности к повседневной работе с такими документами, как процедуры, методики, стандарты и т. д. Так как политику безопасности изначально формулировали для другой структуры, возможны определенные сложности с адаптацией повседневных документов.

К неэффективной политике второго типа относится попытка решить задачу не принятием общих стратегических планов, а путем сиюминутных решений.

Например, системный администратор, устав от того, что пользователи своими неосторожными манипуляциями нарушают работу сети, предпринимает следующие действия: берет лист бумаги и за десять минут набрасывает правила (что можно, а что нельзя, кому разрешен доступ к данным определенного свойства, а кому – нет) и озаглавливает это «Политикой». Если руководство такую «Политику» утверждает, то она впоследствии может годами служить основой деятельности структуры в сфере информационной безопасности, создавая ощутимые проблемы: например, с внедрением новых технологий не всегда поставишь и необходимое программное обеспечение. В итоге начинают допускаться исключения из правил (например, нужна какая-то программа, она дорогостоящая, и работник убеждает руководство использовать нелегальную версию вопреки ранее установленным правилам безопасности), что сводит на нет всю защиту.

Разработка эффективной системы информационной безопасности

Для создания эффективной системы информационной безопасности должны быть разработаны:

- концепция информационной безопасности (определяет в целом политику, ее принципы и цели);
- стандарты (правила и принципы защиты информации по каждому конкретному направлению);
- процедура (описание конкретных действий для защиты информации при работе с ней: персональных данных, порядка доступа к информационным носителям, системам и ресурсам);
- инструкции (подробное описание того, что и как делать для организации информационной защиты и обеспечения имеющихся стандартов).

Все вышеприведенные документы должны быть взаимосвязаны и не противоречить друг другу.

Также для эффективной организации информационной защиты следует разработать аварийные планы. Они необходимы на случай восстановления информационных систем при возникновении форс-мажорных обстоятельств: аварий, катастроф и т. д.

Структура концепции защиты

Сразу заметим: концепция информационной защиты не тождественна стратегии. Первая статична, в то время как вторая – динамична.

Основными разделами концепции безопасности являются:

- определение ИБ;
- структура безопасности;
- описание механизма контроля над безопасностью;
- оценка риска;
- безопасность информации: принципы и стандарты;
- обязанности и ответственность каждого отдела, управления или департамента в осуществлении защиты информационных носителей и прочих данных;
- ссылки на иные нормативы о безопасности.

Помимо этого не лишним будет раздел, описывающий основные критерии эффективности в сфере защиты важной информации. Индикаторы эффективности

защиты необходимы, прежде всего, топ-менеджменту. Они позволяют объективно оценить организацию безопасности, не углубляясь в технические нюансы. Ответственному за организацию безопасности также необходимо знать четкие критерии оценки эффективности ИБ, дабы понимать, каким образом руководство будет оценивать его работу.

Перечень основных требований к документации по безопасности

Политику безопасности надо формулировать с учетом двух основных аспектов:

1. Целевая аудитория, на которую рассчитана вся информация по безопасности – руководители среднего звена и рядовые сотрудники не владеют специфической технической терминологией, но должны при ознакомлении с инструкциями понять и усвоить предоставляемую информацию.

2. Инструкция должна быть лаконичной и при этом содержать всю необходимую информацию о проводимой политике. Объемный «фолиант» никто подробно изучать не будет, а тем более запоминать.

Из выше перечисленного вытекают и два требования к методическим материалам по безопасности:

- они должны быть составлены простым русским языком, без использования специальных технических терминов;
- текст по безопасности должен содержать цели, пути их достижения с указанием назначения меры ответственности за несоблюдение ИБ. Все! Никакой технической или иной специфической информации.

Организация и внедрение ИБ

После того, как документация по информационной безопасности готова, необходима плановая организация работы по ее внедрению в повседневную работу. Для этого необходимо:

- ознакомить коллектив с утвержденной политикой обработки информации;
- знакомить с данной политикой обработки информации всех новых работников (например, проводить информационные семинары или курсы, на которых предоставлять исчерпывающие разъяснения);
- тщательно изучить имеющиеся бизнес-процессы ради обнаружения и минимизации рисков;
- активно участвовать в продвижении новых бизнес-процессов, дабы не стать безнадежно отстающим в сфере ИБ;
- составить подробные методические и информационные материалы, инструкции, дополняющие политику обработки информации (например, правила предоставления доступа к работе в Интернете, порядок входа в помещения с ограниченным доступом, перечень информационных каналов, по которым можно передавать конфиденциальные данные, инструкция по работе с информсистемами и т. д.);
- раз в три месяца пересматривать и корректировать доступ к информации, порядок работы с ней, актуализировать принятую по ИБ документацию, постоянно мониторить и изучать существующие угрозы ИБ.

Лица, пытающиеся получить несанкционированный доступ к информации

В заключение мы классифицируем тех, кто может или хочет получить несанкционированный доступ к информации.

Потенциальные внешние нарушители:

1. Посетители офиса.
2. Ранее уволенные сотрудники (особенно те, кто ушел со скандалом и знает, как получить доступ к информации).
3. Хакеры.
4. Сторонние структуры, в том числе конкуренты, а также криминальные группировки.

Потенциальные внутренние нарушители:

1. Пользователи компьютерной техники из числа сотрудников.
2. Программисты, системные администраторы.
3. Технический персонал.

Для организации надежной защиты информации от каждой из перечисленных групп требуются свои правила. Если посетитель может просто забрать с собой какой-то листок с важными данными, то человек из техперсонала – создать незарегистрированную точку входа и выхода из ЛВС. Каждый из случаев – утечка информации. В первом случае достаточно выработать правила поведения персонала в офисе, во втором – прибегнуть к техническим средствам, повышающим информационную безопасность, таким как DLP-системы и SIEM-системы, предотвращающие утечки из компьютерных сетей.

При разработке ИБ надо учитывать специфику перечисленных групп и предусмотреть действенные меры предотвращения утечки информации для каждой из них.

4. Система управления информационной безопасностью организации (СУИБ)

Управление информационной безопасностью выходит далеко за рамки централизованного удаленного управления антивирусами и другими решениями, обеспечивающими защиту информации. Менеджмент ИБ – это не просто централизованный контроль над своевременным обновлением антивирусных баз, регулярным антивирусным сканированием и выполнением на клиентской стороне других задач, связанных с информационной безопасностью. Это важная часть менеджмента всей организации, обеспечивающая эффективность процессов и решающая не только тактические, но и стратегические задачи.

Основные функции систем управления информационной безопасностью (СУИБ) – это:

- выявление и анализ рисков информационной безопасности
- планирование и практическая реализация процессов, направленных на минимизацию рисков ИБ
- контролирование этих процессов
- внесение в процессы минимизации информационных рисков необходимых корректировок.

Качественное управление информационной безопасностью базируется на следующих принципах:

– комплексный подход – управление ИБ должно быть всеобъемлющим, охватывать все компоненты ИС и учитывать все актуальные рискообразующие факторы, действующие в информационной системе предприятия или госучреждения и за их пределами

- согласованность с задачами и стратегией организации
- высокий уровень управляемости
- адекватность используемой и генерируемой информации
- эффективность – оптимальный баланс между возможностями, производительностью и издержками СУИБ
- непрерывность управления
- процессный подход – связывание процессов управления в замкнутый цикл планирования, внедрения, проверки, аудита и корректировки, и поддержание неразрывной связи между этапами цикла, что позволяет сохранять и постоянно повышать качество СУИБ

Основными целями информационной безопасности являются:

- *конфиденциальность информации*, т.е. необходимость введения ограниченной доступности к данной информации для определенного круга лиц;
- *невозможность несанкционированного доступа к информации*, т.е. ознакомления с конфиденциальной информацией посторонних лиц;
- *целостность информации и связанных с ней процессов (создание, ввод, обработка и вывод)*, которая заключается в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию);
- *доступность информации*, т.е. способность обеспечивать своевременный и беспрепятственный доступ лиц к интересующей их информации;
- *минимизация рисков информационной безопасности путем выполнения компенсационных мероприятий*;
- *учет всех процессов, связанных с рисками*.

Достижение заданных целей осуществляется в ходе решения следующих задач:

- ввода в систему терминов информационной безопасности;
- классификации информационных ресурсов предприятия;
- определения владельцев процессов, ответственных за информационную безопасность;
- разработки спектра рисков информационной безопасности и проведения их экспертных оценок;
- определения группы доступа к информационным ресурсам;
- разработки системы управления рисками информационной безопасности (методы и их оценка);
- составления перечней административных и технических мероприятий для минимизации и компенсации рисков;
- осуществления мероприятий информационной безопасности и периодического контроля за состоянием рисков;
- обеспечения физической безопасности и безопасности персонала;
- разработки требований к информационной системе с точки зрения информационной безопасности;

- контроллинга информационной безопасности на предприятии.

Выделяются четыре стадии реализации системы управления информационной безопасностью:

- 1) формирование политики в области рисков;
- 2) анализ бизнес-процессов;
- 3) анализ рисков;
- 4) формирование целевой концепции.

Формирование политики в области рисков подразумевает определение принципов управления ими для всего предприятия в целом. Эти принципы базируются на целях предприятия, его стратегии, также на требованиях, предъявляемых законом и стандартами в области информационной безопасности. Фактором эффективности системы управления информационной безопасностью является ее построение на базе международных стандартов ISO/IEC 17799:2005 и ISO/IEC 27001:2005.

Стандарт ISO/IEC 17799:2005 определяет принципы и является руководством по разработке, внедрению, сопровождению и улучшению системы управления информационной безопасностью, а также описывает механизмы определения целей контроля и его средств в следующих областях:

- политика безопасности (установление принципов управления и средств обеспечения защиты информации);
- управление непрерывностью бизнес-процессов (предотвращение вмешательства в деловые операции и защита процессов обработки информации от последствий серьезных неисправностей или катастроф);
- соблюдение правовых норм (исключение нарушений уголовного и гражданского права, установленных законом обязательств, регулятивных или контрактных обязательств, а также требований по безопасности);
- организация активов и ресурсов (управление защитой информации внутри организации);
- физическая безопасность и безопасность окружающей среды (предотвращение несанкционированного доступа, повреждения и проникновения в служебные помещения или вмешательства в деловую информацию);
- классификация и управление активами (выявление и защита информационных активов);
- защита персонала (снижение рисков, связанных с ошибкой оператора, кражей, мошенничеством или злоупотреблением оборудованием);
- управление доступом (контроль доступа к информации);
- управление средствами связи и эксплуатацией оборудования (корректное и безопасное функционирование средств обработки информации);
- разработка и обслуживание систем (внедрение средств защиты в информационные системы).

Стандарт ISO/IEC 27001:2005 устанавливает требования к системе управления информационной безопасностью предприятия, является руководством по определению, минимизации и управлению опасностями и угрозами, которым может подвергаться информация, и разработан в целях обеспечения помощи в выбо-

ре эффективных и адекватных средств для его защиты. Применение стандарта ISO/IEC 27001:2005 на предприятии позволяет:

- установить требования и цели в области информационной безопасности;
- гарантировать уверенность в том, что управление рисками в области информационной безопасности является эффективным, а также то, что деятельность предприятия соответствует законодательству и другим нормативным документам;
- реализовать процесс контроля за внедрением системы управления информационной безопасностью;
- идентифицировать и отслеживать существующие процессы управления информационной безопасностью;
- руководству предприятия определить состояние процессов управления защитой информации;
- внутренним и внешним аудиториям установить уровень соответствия политики безопасности регламентам;
- обеспечить партнеров и поставщиков соответствующей информацией о стандартах, процедурах и политике предприятия.

Модель системы информационной безопасности предприятия – это совокупность внешних и внутренних факторов, их влияние на состояние информационной безопасности предприятия и обеспечение сохранности ресурсов. На рис. 9.5 приводится модель системы информационной безопасности предприятия, в которой представлены направления воздействия между следующими факторами:

- угрозами информационной безопасности, которые характеризуются вероятностью возникновения и реализации;
- уязвимостью системы информационной безопасности, влияющей на вероятность реализации угрозы;
- рисками, отражающими предполагаемый ущерб в результате реализации угрозы информационной безопасности.

Информация и материальные ресурсы, которые необходимо защищать, называются *объектами защиты*. К ним относятся:

- речевая информация;
- информация, хранимая и обрабатываемая посредством средств связи в виде различных носителей;
- документы на бумажных носителях;
- технические средства связи и информатизации;
- помещения, предназначенные для обсуждения, обработки и хранения информации;
- информационные системы в целом, включая системы связи;
- документация на технические и программные средства связи и информатизации;
- программные средства.

Под *физическими видами* нарушений подразумеваются повреждение аппаратных средств автоматизированных систем, линий связи и коммуникационного оборудования, кражи или несанкционированное ознакомление с содержанием носителей информации, их хищение.

К *радиоэлектронным видам* нарушений относятся внедрение электронных устройств перехвата информации, получение информации путем перехвата и дешифрования информационных потоков, фотографирование мониторов, навязывание ложной информации в локальных вычислительных сетях, передаче данных и линиях связи.

Для противодействия угрозам и пресечения нарушений на предприятиях организуется процесс управления рисками, который является основой системы информационной безопасности предприятия.

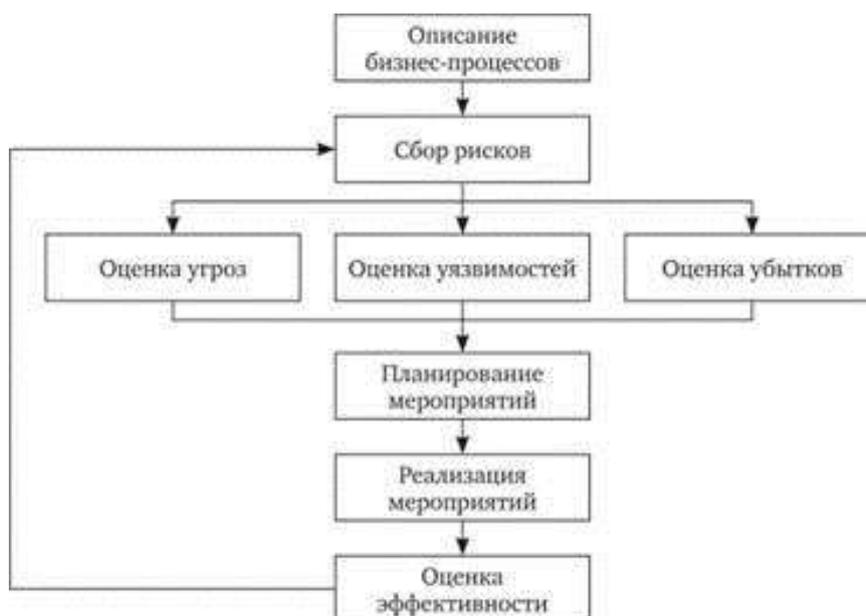
Построение эффективной системы информационной безопасности – это комплексный процесс, направленный на минимизацию внешних и внутренних угроз при учете ограничений на ресурсы и время.

С точки зрения процессного подхода систему информационной безопасности предприятия можно представить как процесс управления рисками, который включает в себя следующие составляющие.

1. *Описание бизнес-процессов.* Выполняется корректировка и анализ бизнес-процессов. По критериям, которые определяются в ходе формирования политики в области рисков, осуществляется идентификация бизнес-процессов.

2. *Сбор рисков.* Проводится для выявления степени подверженности предприятия угрозам, которые могут нанести существенный ущерб. Для этого осуществляется анализ его бизнес

процессов и опрос экспертов предметной области. Результатом (выходом) данного процесса считается классификационный перечень всех потенциальных рисков.



Модель процесса управления рисками для системы информационной безопасности

К стандартным рискам информационной безопасности относятся:

- изъятие конфиденциальной информации с локальных мест;
- преднамеренное изменение информации с целью уничтожения;
- копирование важных документов и передача конкуренту;
- незаконное проникновение в корпоративную сеть;
- уничтожение по техническим причинам.

3. *Оценка рисков.* Определяются характеристики рисков и ресурсы информационной системы. Основным результатом (выходом) данного процесса является перечень всех потенциальных рисков с их количественными и качественными оценками ущерба и возможности реализации, а дополнительным – перечень рисков, которые не будут отслеживаться на предприятии.

Процесс оценки рисков состоит из следующих шагов:

- описание объекта и мер защиты;
- идентификация ресурса и определение его количественных показателей;
- анализ угроз информационной безопасности;
- оценка уязвимостей;
- оценка существующих и предполагаемых средств обеспечения информационной безопасности.

4. *Планирование мероприятий.* Целью планирования мероприятий по минимизации рисков является определение сроков и перечня работ по исключению или минимизации ущерба в случае минимизации риска.

Выделяются следующие виды мероприятий по информационной безопасности:

- организационные;
- правовые;
- организационно-технические;
- программные;
- инженерно-технические.

5. *Реализация мероприятий.* Под реализацией мероприятий по минимизации рисков подразумеваются выполнение запланированных работ, контроль качества полученных результатов и сроков. Результатом данного процесса являются выполненные работы по минимизации рисков и время их проведения.

6. *Оценка эффективности.* Оценка эффективности системы управления информационной безопасностью – это системный процесс получения и оценки объективных данных о текущем состоянии системы, действиях и событиях, происходящих в ней, устанавливающий уровень их соответствия определенным критериям.

Целями процесса являются:

- оценка текущего уровня эффективности системы;
- локализация «узких» мест в системе;
- оценка соответствия системы предприятия существующим стандартам в области информационной безопасности;
- выработка рекомендаций и регламентов по обеспечению безопасности объектов защиты.

Результаты процесса могут использоваться в целях аудита для подготовки предприятия к сертификации по стандарту ISO/ IEC 27001:2005.

5. Ресурсное обеспечение СУИБ.

Для полноценной деятельности служб информационной безопасности необходимы *следующие виды ресурсов*:

финансовые – для закупки средств защиты информации, вспомогательного оборудования, капитального строительства, ремонта средств защиты и оборудования, оплаты сотрудников, для покрытия других затрат;

материальные – представляют некоторые объекты финансовых вложений, и поэтому тесно взаимоувязаны с первым видом ресурсного обеспечения, а именно к ним можно отнести стройматериалы, мебель, сейфы, запасные части и инструменты и некоторые другие;

технические – аппаратные средства защиты информации, технические средства охраны и контроля, автотранспорт, автономные источники питания и прочие;

энергетические – потребляемые объемы электроэнергии, горюче-смазочные материалы для автотранспорта и автономных источников питания;

информационные – к этому классу ресурсов можно отнести программные продукты, нормативно-методическую, специальную литературу, электронные базы данных, знания специалистов, необходимые для эффективного выполнения функций защиты;

временные – заключаются во временных затратах на выполнение тех или иных процедур защиты, анализ временных ресурсов активно используется при создании оргштатных проектов служб защиты, в которых учитывается общий временной объем процесса защиты, относительно стандартизированного объема, реализуемого одним сотрудником;

пространственные – необходимы для обеспечения контролируемых зон вокруг объектов ТСПИ, информационных коммуникаций, размещения средств и технологических участков защиты данных, создания имплицативных зон защиты.

Достаточно очевидно, что *главным видом ресурсного обеспечения является финансовое*. С помощью его можно решать задачи всех остальных ресурсных вложений. Поэтому, возвращаясь к материалу второй главы, подчеркнем важность оценки проекта системы защиты по критерию «стоимость информации – стоимость защиты», то есть проект системы защиты не должен быть дороже самой информации.

6. Контроль и проверка процессов УИБ.

Как и любой вид деятельности, информационная безопасность подлежит контролю и периодической переоценке, чтобы гарантировать адекватность (соответствие) политик и средств (методов) контроля поставленным целям.

Контролировать факторы, влияющие на риски и указывающие на эффективность информационной безопасности

Контроль должен быть сосредоточен, прежде всего, на (1) наличии средств и методов контроля и их использования, направленного на уменьшение рисков и (2) оценке эффективности программы и политик информационной безопасности, улучшающих понимание пользователей и сокращающих количество инцидентов. Такие проверки предусматривают тестирование средств (методов) контроля, оценку их соответствия политикам организации, анализ инцидентов безопасности, а также другие индикаторы эффективности программы информационной безопасности. Эффективность работы руководящей группы может быть оценена, основываясь, например, на следующих показателях (но, не ограничиваясь ими):

- число проведенных тренингов и встреч;
- число выполненных оценок риска (рисков);
- число сертифицированных специалистов;
- отсутствие инцидентов, затрудняющих работу сотрудников организации;
- снижение числа новых проектов, внедренных с задержкой из-за проблем информационной безопасности;
- полное соответствие или согласованные и зарегистрированные отклонения от минимальных требований информационной безопасности;
- снижение числа инцидентов, влекущих за собой несанкционированный доступ, потерю или искажение информации.

Использовать полученные результаты для координации будущих усилий и повышения ответственности менеджмента

Контроль, безусловно, позволяет привести организацию в соответствие с принятыми политиками информационной безопасности, однако полные выгоды от контроля не будут достигнуты, если полученные результаты не используются для улучшения программы обеспечения информационной безопасности. Анализ результатов контроля предоставляет специалистам в области информационной безопасности и менеджерам бизнес-подразделений средства (1) переоценки ранее идентифицированных рисков, (2) определения новых проблемных участков, (3) переоценки достаточности и уместности существующих средств и методов контроля (управления) и действий по обеспечению информационной безопасности, (4) определения потребностей в новых средствах и механизмах контроля, (5) переадресации контрольных усилий (контролирующих действий). Кроме того, результаты могут использоваться для оценки деятельности бизнес-менеджеров, ответственных за понимание и уменьшение рисков в бизнес-подразделениях.

Отслеживать новые методы и средства контроля

Важно гарантировать, что (1) специалисты в области информационной безопасности не «отстают» от разрабатываемых методов и инструментов (приложений) и располагают самой последней информацией об уязвимости информационных систем и приложений, (2) высший менеджмент гарантирует, что располагает для этого необходимыми ресурсами.