ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА
(РОСАВИАЦИЯ)

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ» (МГТУ ГА)

Кафедра основ радиотехники и защиты информации

С.П. Матыюк

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

**Учебное пособие**

*Утверждено редакционно-издательским советом МГТУ ГА в качестве учебного пособия*

Москва
ИД Академии Жуковского
2024

УДК 004.056
ББК 001.8
М34

Печатается по решению редакционно-издательского совета
Московского государственного технического университета ГА

Рецензенты:
*Петров В.И.* (МГТУ ГА) – канд. техн. наук;
*Автаев С.В.* (ООО «СОФТ – Горизонт») – канд. техн. наук

**Матыюк С.П.**

М34 Информационная безопасность [Текст] : учебное пособие / С.П. Матыюк. – М. : ИД Академии Жуковского, 2024. – 64 с.

ISBN 978-5-907863-47-7

В учебном пособии «Информационная безопасность» рассматривается комплекс вопросов, связанных с введением в информационную безопасность, а также с ее управлением.

В работе рассматриваются такие вопросы, как: основы законодательства РФ в области информационной безопасности, перечень программных средств обеспечения информационной безопасности. Большое внимание уделяется защитным механизмам, используемых в информационных системах.

Учебное пособие разработано для студентов II курса 4 семестра очной формы обучения по направлению подготовки 25.05.05 «Эксплуатация воздушных судов и организация воздушного движения», квалификация (степень) – инженер.

Рассмотрено и одобрено на заседаниях кафедры 16.04.2024 г. и методического совета 23.04.2024 г.

**УДК 004.056**
**ББК 001.8**
Св. тем. план 2024 г.
поз. 18

МАТЫЮК Сергей Петрович

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебное пособие

*В авторской редакции*

Подписано в печать 20.11.2024 г.
Формат 60х84/16 Печ. л. 4 Усл. печ. л. 3,72
Заказ № 1038/0909-УП04 Тираж 30 экз.

Московский государственный технический университет ГА
125993, Москва, Кронштадтский бульвар, д. 20

Издательский дом Академии имени Н. Е. Жуковского
125167, Москва, 8-го Марта 4-я ул., д. 6А
Тел.: (499) 755-55-43 E-mail: zakaz@itsbook.ru

**ISBN 978-5-907863-47-7**

## Введение

Современный специалист в области авиационных технологий должен обладать знаниями и навыками обеспечения информационной безопасности (ИБ). Связано это с тем, что в информационных системах предприятий и организаций, а также на воздушных судах хранится и обрабатывается критически важная информация, для которой нарушение конфиденциальности, целостности или доступности может привести к нежелательным последствиям. Поэтому вопросам обеспечения информационной безопасности должно уделяться внимание на всех этапах разработки и эксплуатации информационных систем.

В данном учебном пособии изложен материал учебной дисциплины «Информационная безопасность», в ходе изучения которой студенты получают базовые знания о теории защиты информации, методах и средствах обеспечения информационной безопасности, а также практические навыки организации защиты информационных систем. Пособие включает в себя три раздела.

В разделе 1 «Введение в информационную безопасность» приводятся базовые понятия, связанные с обеспечением информационной безопасности, рассматриваются основные угрозы безопасности и меры противодействия им. Раскрываются основные направления криптографии, рассматриваются вопросы защиты информации в IP сетях, беспроводных сетях, базах данных.

В разделе 2 «Защитные механизмы, используемые в информационных системах» изучаются состав и принципы работы системы обнаружения вторжений, систем защиты внутреннего информационного периметра, а также центра управления информационной безопасностью.

В разделе 3 «Управление информационной безопасностью» раскрываются состав и принципы функционирования систем управления информационной безопасностью. Излагаются основные политики информационной безопасности. Проводится анализ и управление рисками ИБ. Рассматриваются основные кадровые и организационные вопросы информационной безопасности.

# Раздел 1. ВВЕДЕНИЕ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

## 1. Теоретические основы информационной безопасности.

### 1.1 Базовые понятия

Введем определения ряда базовых понятий.

***Информация*** – это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. Информация может существовать в различных формах в виде совокупностей некоторых знаков (символов, сигналов и т. д.) на носителях различных типов. Она может представлять ценность для отдельных лиц или организаций.

Информация обладает следующими свойствами:

- ценность;
- конфиденциальность;
- целостность;
- доступность;
- концентрация;
- рассеяние;
- сжатие.

Основными свойствами являются конфиденциальность, целостность и доступность.

***Конфиденциальность*** – субъективно определяемая характеристика информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к информации.

***Целостность*** информации – свойство информации существовать в неискаженном виде. Обычно интересует обеспечение более широкого свойства – достоверности информации, которое складывается из адекватности (полноты и точности) отображения состояния предметной области.

***Доступность*** информации – свойство системы, в которой циркулирует информация, обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность к обслуживанию поступающих от субъектов запросов, когда в обращении к ним возникает необходимость.

***Защищаемая информация*** – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственниками информации. Собственниками информации могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо [1].

В настоящее время, большинство информации, в том числе и критически важной для отдельных людей или организаций, хранятся, обрабатываются и передаются с использованием автоматизированных систем (АС) обработки информации.

***Система обработки информации*** – совокупность технических средств и программного обеспечения, а также методов обработки информации и действий персонала, необходимых для выполнения автоматизированной обработки информации [2].

***Объект информатизации*** – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

В зависимости от конкретных условий, может решаться задача обеспечения комплексной безопасности объекта информатизации или защиты отдельных ресурсов – информационных, программных и т. д.

***Информационные ресурсы (активы)*** – отдельные документы и отдельные массивы документов, документы и массивы документов, содержащиеся в информационных системах (библиотеках, архивах, фондах, банках данных, информационных системах других видов).

Рассматривая вопросы безопасности, АС, можно говорить о наличии некоторых «желательных» состояний системы, через которые и описывается ее «защищенность» или «безопасность». Безопасность является таким же свойством системы, как надежность или производительность, и в последнее время ей уделяется все большее внимание. Чтобы указать на причины выхода системы из безопасного состояния, вводятся понятия «угроза» и «уязвимость».

***Угроза (безопасности информации)*** – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

***Источник угрозы безопасности информации*** – субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации. По типу источника угрозы делят на связанные и несвязанные с деятельностью человека. Примерами могут служить удаление пользователем файла с важной информацией и пожар в здании, соответственно. Угрозы, связанные с деятельностью человека, разделяют на угрозы случайного и преднамеренного характера. В последнем случае источник угрозы называют нарушителем или злоумышленником.

***Уязвимость (информационной системы)*** – свойство информационной системы, обуславливающее возможность реализации угроз безопасности обрабатываемой в ней информации. Например, угроза потери информации из-за сбоя в сети электропитания может реализоваться, если в АС не применяются источники бесперебойного питания или средства резервного электроснабжения (это является уязвимостью).

Если говорить об информационных ресурсах, то реализация угрозы может привести к таким последствиям, как получение информации людьми, которым она не предназначена, уничтожение или изменение информации, недоступность ресурсов для пользователей. Таким образом, мы подошли к определению трех основных угроз безопасности, которые тесно связаны с основными свойствами информации.

***Угроза конфиденциальности*** (угроза раскрытия) – это угроза, в результате реализации которой, конфиденциальная информация становится доступной лицу, группе лиц или какой-либо организации, которой она не предназначалась.

***Угроза целостности*** – угроза, в результате реализации которой информация становится измененной или уничтоженной. Необходимо отметить, что и в нормальном режиме работы АС данные могут изменяться и удаляться. Являются ли эти действия легальными или нет, должно определяться политикой безопасности.

***Политика безопасности*** – совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

***Угроза отказа в обслуживании*** (угроза доступности) – угроза информационной безопасности, реализация которой приведет к отказу в обслуживании клиентов АС, несанкционированному использованию ресурсов злоумышленниками по своему усмотрению.

Таким образом, безопасность информации – это состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность. А защита информации может быть определена как деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Выделяются следующие направления защиты информации:

- правовая защита информации – защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите

информации, применение этих документов (актов), а также надзор и контроль за их исполнением;

- техническая защита информации – защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств;

- криптографическая защита информации – защита информации с помощью ее криптографического преобразования;

- физическая защита информации – защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

## 2. Основные направления криптографии

### 2.1. Основные понятия и определения криптографии

Рассмотрим основные понятия, принятые в криптографии [3], и вначале определим понятие криптографии.

***Криптография*** — это раздел прикладной математики (криптологии), изучающий модели, методы, алгоритмы, программные и аппаратные средства преобразования информации (шифрования) в целях сокрытия ее содержания, предотвращения видоизменения или несанкционированного использования. На решение взаимообратных задач нацелен криптоанализ. ***Криптоанализ*** — это раздел прикладной математики (криптологии), изучающий модели, методы, алгоритмы, программные и аппаратные средства анализа криптосистем или их входных и выходных сигналов с целью извлечения конфиденциальных параметров, включая открытый текст. Таким образом, криптография и криптоанализ составляют единое целое и образуют науку - ***криптологию,*** которая с самого начала развивалась как двуединая наука.

Исторически центральным понятием криптографии является понятие шифра. ***Шифром*** называется совокупность обратимых криптографических преобразований множества открытых текстов на множество зашифрованных текстов, проводимых с целью их защиты. Конкретный вид криптографического преобразования открытого текста определяется с помощью ***ключа*** шифрования. ***Открытым текстом*** называют исходное сообщение, которое подлежит зашифрованию. Под ***зашифрованием*** понимается процесс применения обратимого криптографического преобразования к открытому тексту, а

результат этого преобразования называется ***шифртекстом*** или ***криптограммой***. Соответственно, процесс обратного криптографического преобразования криптограммы в открытый текст называется ***расшифрованием***.

Расшифрование нельзя путать с дешифрованием. ***Дешифрование*** (***дешифровка***, ***взлом***) - процесс извлечения открытого текста без знания криптографического ключа на основе перехваченных криптограмм. Таким образом, расшифрование проводится законным пользователем, знающим ключ шифра, а дешифрование - криптоаналитиком.

***Криптографическая система*** - семейство преобразований шифра и совокупность ключей. Само по себе описание криптографического алгоритма не является криптосистемой. Чтобы описание стало системой, его необходимо дополнить схемами распределения и управления ключами.

Классификация криптосистем представлена на рис. 2.1.

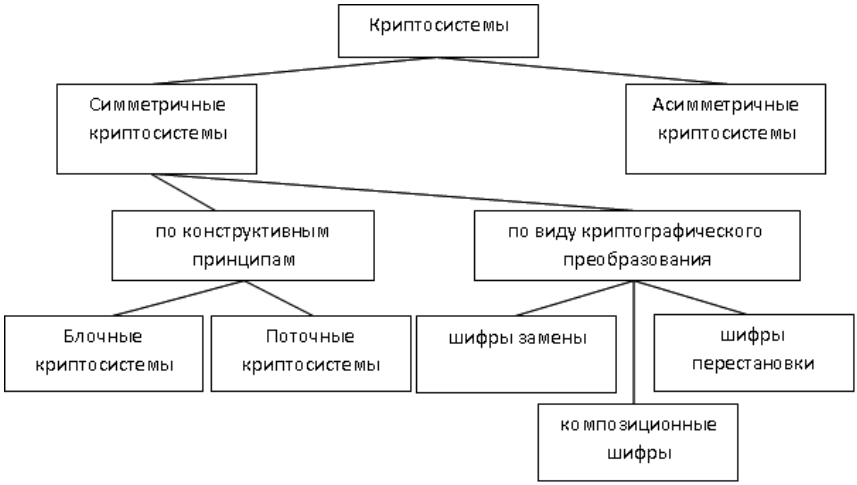


Рис. 2.1. Классификация криптосистем

*Симметричные криптосистемы (криптосистемы с секретным ключом)* построены на принципе сохранения в тайне ключа шифрования. На рис. 2.2 представлена упрощенная структурная схема симметричной криптосистемы. Перед использованием симметричной криптосистемы пользователи должны получить общий секретный ключ $k$ и исключить доступ к нему

злоумышленника. Открытое сообщение $X$ подвергается криптографическому преобразованию $f_k(X)$ и полученная криптограмма $Y$ по открытому каналу связи передается получателю, где осуществляется обратное преобразование $f_k^{-1}(Y)$ с целью выделения исходного открытого сообщения $X$.

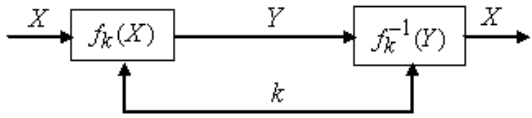


Рис. 2.2. Упрощенная структурная схема симметричной криптосистемы

Симметричные криптосистемы классифицируются по различным признакам[6-8]: по виду криптографического преобразования; по конструктивным принципам; по виду защищаемой информации; по криптографической стойкости и т. д. Чаще всего используются первые два признака классификации. В связи с этим множество симметричных криптосистем делится:

- по виду криптографического преобразования – на шифры перестановки, шифры замены и композиционные шифры;
- по конструктивным принципам – на поточные криптосистемы и блочные криптосистемы.

Под ***шифром перестановки*** понимается переупорядочение букв исходного сообщения, в результате которого он становиться нечитаемым. Под ***шифром замены*** понимается преобразование, которое заключается в замене букв исходного сообщения на другие буквы по более или менее сложному правилу. ***Композиционные шифры*** строятся на основе шифров замены и перестановки. ***Блочные симметричные криптосистемы*** (БСК) представляют собой семейство обратимых криптографических преобразований блоков исходного сообщения. ***Поточные криптосистемы*** (ПСК) преобразуют посимвольно исходное сообщение в криптограмму.

Отличительной особенностью ***асимметричных криптосистем (криптосистем с открытым ключом)*** является то, что для зашифрования и расшифрования информации используются разные ключи. На рис. 2.3 представлена упрощенная структурная схема асимметричной криптосистемы. Криптосистема с открытым ключом определяется тремя алгоритмами: генерацией ключей, шифрованием и расшифрованием. Алгоритм генерации

ключей позволяет получить пару ключей $(k_o, k_з)$, причем $k_o \neq k_з$. Один из ключей $k_o$ публикуется, он называется ***открытым***, а второй $k_з$, называется ***закрытым*** (или секретным) и храниться в тайне. Алгоритмы шифрования $f_{k_o}(\cdot)$ и расшифрования $f_{k_з}^{-1}(\cdot)$ таковы, что для любого открытого текста $X$ выполняется равенство $f_{k_з}^{-1}(f_{k_o}(X)) = X$.

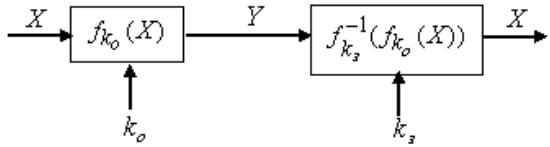


Рис. 2.3. Упрощенная структурная схема асимметричной криптосистемы

*Ассиметричные криптосистемы (с открытым ключом)* делятся на следующие виды:

***Криптосистема RSA*** названа была так в честь ее разработчиков: Рона Ривеста (Ron Rivest), Ади Шамира (Adi Shamir) и Леонарда Адлемана (Leonard Adleman). Криптосистема RSA является одной из самых используемых в мире асимметричных криптосистем.

Криптосистема с открытым ключом RSA формально определяется следующим образом [6-9]:

$$RSA = (X, Y, K, x, y, k_O, k_з, N, E, D), \qquad (2.1)$$

где $X$ - множество открытых текстов, $Y$ - множество криптограмм, $K$ - множество ключей, $x \in X$ - некоторый открытый текст, $y \in Y$ - некоторая криптограмма, $k_o \neq k_з$, $(k_o, k_з) \in K$ - ключи шифрования и расшифрования, удовлетворяющие условию $k_o k_з \bmod \varphi(N) = 1$, $N = pq$ - натуральное число, причем $p$ и $q$ - простые числа, $E$ - функция шифрования, $D$ - функция расшифрования.

***Криптосистема Шамира*** была первой криптосистемой с открытым ключом.

Криптосистема Шамира формально определяется следующим образом [6-9]:

$$Shamir = (X, Y, K, x, y, k_o, k_з, p, F), \qquad (2.2)$$

где $X$ - множество открытых текстов, $Y$ - множество криптограмм, $K$ - множество ключей, $x \in X$ - некоторый открытый текст, $y \in Y$ - некоторая криптограмма, $k_o \neq k_з$, $(k_o, k_з) \in K$ - ключи шифрования, удовлетворяющие условию $k_o k_з \bmod(p-1) = 1$, $p$ - большое простое число, $F$ - криптографическая функция.

***Криптосистема Эль Гамаля*** формально определяется следующим образом:

$$ElGamal = (X, Y, K, x, y, k_o, k_з, p, g, E, D), \qquad (2.3)$$

где $X$ - множество открытых текстов, $Y$ - множество криптограмм, $K$ - множество ключей, $x \in X$ - некоторый открытый текст, $y \in Y$ - некоторая криптограмма, $k_o \neq k_з$, $(k_o, k_з) \in K$ - ключи шифрования и расшифрования, удовлетворяющие условию: $k_o = g^{k_з} \bmod p$, $p$ - большое простое число, $g$ - число, такое что, различные степени числа $g$ суть различные числа по модулю $p$, $E$ - функция шифрования, $D$ - функция расшифрования.

Особенностью криптосистемы Эль Гамаля является то, что объем передаваемой криптограммы в два раза превышает объем исходного сообщения.

***Криптосистема с открытым ключом Рабина*** формально определяется следующим образом [6]:

$$Rabin = (X, Y, x, y, N, p, q, E, D), \qquad (2.4)$$

где $X$ - множество открытых текстов, $Y$ - множество криптограмм, $x \in X$ - некоторый открытый текст, $y \in Y$ - некоторая криптограмма, $N = pq$ - RSA-модуль (является открытым ключом криптосистемы), где $p$ и $q$ - секретные ключи криптосистемы, $E$ - функция шифрования, $D$ - функция расшифрования.

***Криптосистемы на эллиптических кривых*** – одно из новых направлений в криптографии. Эллиптические кривые давно изучаются математикой, но их использование в криптографии впервые было предложено Коблицом и Миллером в 1985 году. Прошедшие три десятилетия подтвердили эффективность этих криптосистем и привели к открытию множества их реализаций. Основным достоинством криптосистем на эллиптических кривых является их более высокая стойкость по сравнению с традиционными асимметричными криптосистемами при равных вычислительных затратах.

## 2.2 Электронная подпись

Одна из важнейших проблем, решаемых с использованием асимметричных методов шифрования - проблема подтверждения авторства. Данная проблема возникает при следующих обстоятельствах:

- когда некоторый абонент $m$ получает сообщение, предположительно от абонента $m+1$, необходимо подтвердить, что получено сообщение именно от абонента $m$, а не от третьего лица;
- когда абонент $m$ получает от абонента $m+1$ сообщение, необходимо подтвердить, что оно не было изменено третьим лицом.

Для решения этой проблемы были разработаны алгоритмы электронной подписи. Определение электронной подписи дано федеральным законом № 63-ФЗ от 6.04.2011 г.

***Электронная подпись*** - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Во многих странах мира, в том числе в России, введены в действие стандарты на электронную подпись. Часто используется термин «цифровая подпись». Оба термина означают одно и то же.

Электронная подпись (ЭП) должна обладать следующими свойствами:

1) подписать документ может только законный владелец ЭП;

2) автор ЭП не может от нее отказаться;

3) в случае возникновения спора возможно участи третьих лиц (например, суда) для установления подлинности ЭП.

Из рассмотренных свойств можно определить злонамеренные действия, к которым относятся:

- ***отказ (ренегатство)*** – отправитель впоследствии отказывается от переданного сообщения;
- ***фальсификация*** – получатель (или третье лицо) подделывает сообщение;
- ***изменение*** - получатель (или третье лицо) вносит изменение в сообщение;
- ***маскировка*** – злоумышленник маскируется под легального пользователя.

Схема ЭП включает в себя:

- параметр безопасности $n$;
- пространство исходных сообщений;
- алгоритм $G$ генерации пары ключей $(k_з, k_о)$;
- алгоритм $S$ формирования подписи;
- алгоритм $V$ проверки подписи.

Электронная подпись $s = S(k_з, x)$ называется ***допустимой*** для документа $x$, если она принимается алгоритмом $V$. ***Подделкой*** ЭП документа $x$ называется нахождение злоумышленником, не имеющим секретного ключа, допустимой подписи для документа $x$.

Обобщенная схема ЭП имеет следующий вид (см. рис.2.3) [3-6]:

1. Отправитель А вычисляет $(k_з, k_o) = G(n)$ и посылает получателю В $k_o$.

2. Для получения подписи документа $x$ отправитель вычисляет $s = S(k_з, x)$ и посылает $\langle x, s \rangle$ получателю.

3. Получатель вычисляет $V(x, s, k_o)$ и, в зависимости от результата, принимает или отвергает подпись $s$ отправителя А.

В классической схеме ЭП предполагается, что отправитель знает содержание подписываемого документа, а получатель проверяет подлинность ЭП без какого-либо разрешения и участия отправителя А.

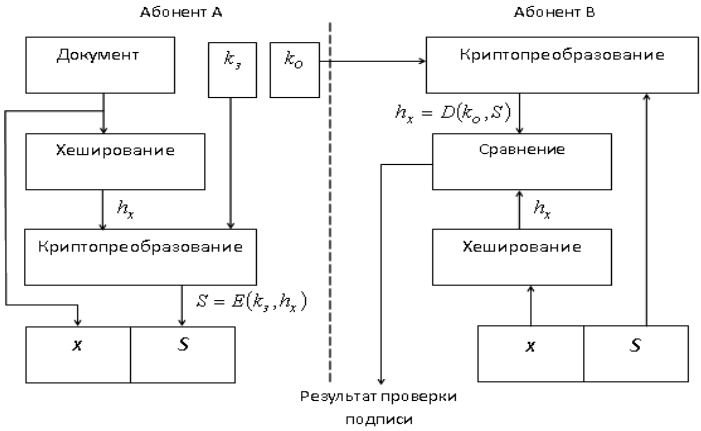


Рис. 2.3. Обобщенная схема формирования и проверки ЭП

При формировании ЭП по классической схеме отправитель А вычисляет хеш-функцию (хеш-образ) документа $h_x = h(x)$ и, при необходимости, дополняет его до требуемой длины. Алгоритм вычисления хеш-функции известен всем абонентам сети. Отметим важные свойства:

1) хеш-функция обеспечивает преобразование входного массива данных любого размера в выходной массив данных (хеш) фиксированного размера;

2) практически невозможно внести изменения во входной массив данных, не изменив выходной массив данных (хеш).

Отправителю А достаточно снабдить подписью не сам документ $x$, а его хеш-образ $h_x$.

## 2.2. Хэш – функция

Хеширование иногда считают видом криптографического преобразования. Вместе с тем, криптографическое преобразование, по определению, является обратимым, а хеширование представляет собой необратимое преобразование.

Для того чтобы хеш-функция могла быть использована в криптографических алгоритмах она должна обладать следующими свойствами [3-7]:

- преобразование $h$ может быть применено к $x$ любого размера;
- выходное значение $h_x$ должно иметь фиксированный размер;
- значение $h_x$ достаточно просто вычисляется для любого $x$;
- для любого значения $h_x$ с вычислительной точки зрения невозможно найти $x$;
- для любого значения $x$ с вычислительной точки зрения невозможно найти $x' \neq x$, такое, что $h(x) = h(x')$;
- значение хеш-функции $h_x$ должно быть чувствительным к любым изменениям входной информационной последовательности $x$.

Если хеш-функция обладает перечисленными свойствами, то она считается качественной. Для качественной хеш-функции три следующие задачи являются вычислительно неразрешимыми.

1. ***Задача нахождения прообраза*** – это задача нахождения входной последовательности $x$ по заданному хеш-образу $h_x$. Хеш-функция должна быть стойкой в смысле обращения.

2. ***Задача нахождения коллизий*** – это задача нахождения последовательностей $x'$ и $x''$, причем $x' \neq x''$, для которых $h(x') = h(x'')$. Хеш-функция должна быть стойкой в смысле нахождения коллизий.

3. ***Задача нахождения второго прообраза*** – это задача нахождения для заданной входной последовательности $x$ другой входной последовательности $x'$, причем $x' \neq x$, такой, что $h(x) = h(x')$. Эта задача является разновидностью задачи нахождения коллизий.

## 3. Защита информации в IP сетях

На сегодняшний день стек сетевых протоколов TCP/IP является наиболее широко используемым как в глобальных, так и в локальных компьютерных сетях. Именно поэтому методы и средства защиты передаваемых данных в IP-сетях представляют особый интерес [10].

Далее будут рассмотрены криптографические протоколы, позволяющие защищать электронную почту, передаваемые данные на транспортном и сетевом уровнях (рис. 3.1).

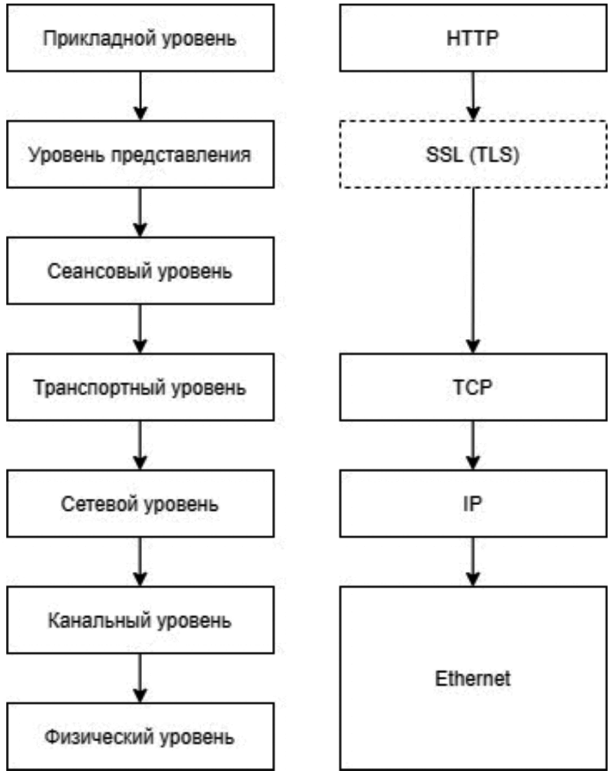


Рис. 3.1. Сетевая модель OSI

## 3.1. Протокол защиты электронной почты S/MIME

Протокол Secure Multipurpose Internet Mail Extensions (S/MIME) предназначен для защиты данных, передаваемых в формате MIME, в основном по электронной почте.

Результатами фиксации указанной информации становятся одна или несколько записей в оперативной базе данных. Сам процесс фиксации называют ***бизнес-транзакцией***, а информацию — ***данными транзакции***. Исходя из определения, транзакция — это последовательность операторов манипулирования данными, выполняющаяся как единое целое и переводящая базу данных из одного целостного состояния в другое целостное состояние.

Протокол S/MIME предоставляет следующие криптографические услуги безопасности (криптографичекие сервисы):

- проверка целостности сообщения;
- установление подлинности отправителя (аутентификация);
- обеспечение секретности передаваемых данных (шифрование).

Нужно отметить, что сам по себе формат MIME описывает порядок форматирования писем, содержащих различные типы данных (обычный текст, текст в формате html, видео и графические файлы различных типов и т. д.). При использовании S/MIME добавляются новые типы. Это позволяет указать на то, что данные в этом разделе являются зашифрованными, подписанными и т. д. Протокол позволяет обычным почтовым клиентам защищать исходящую почту и интерпретировать криптографические сервисы, добавленные во входящую почту (расшифровывать сообщения, проверять их целостность и т. д.). Стандарт определяет использование симметричных криптоалгоритмов для шифрования содержимого почтовых сообщений и алгоритма с открытым ключом для защиты передаваемого вместе с письмом ключа симметричного шифрования.

Протокол S/MIME позволяет использовать различные криптоалгоритмы, причем их список может расширяться. Изначально, из симметричных шифров могли использоваться RC2, DES или TripleDES. Для формирования дайджестов – алгоритмы MD5 и SHA1, причем версия 3 стандарта рекомендует использовать именно последний алгоритм (из-за того, что он формирует более длинный дайджест и считается более надежным). Защита симметричного ключа шифрования и ЭЦП в версии 2 осуществляется с помощью алгоритма RSA с ключом от 512 до 1024 бит. Версия 3 добавляет возможность использовать другие алгоритмы, например алгоритм Диффи-Хеллмана с ключом длиной до 2048 бит. Распределение и аутентификация открытых ключей производится с помощью цифровых сертификатов формата X.509. Таким образом, чтобы защищать переписку с помощью этого протокола, оба абонента должны

сгенерировать ключевые пары и удостоверить открытые ключи с помощью сертификатов.

## 3.2. Протоколы SSL и TLS

Протокол Secure Sockets Layer (SSL) был разработан для обеспечения аутентификации, целостности и секретности трафика на сеансовом уровне модели OSI. В январе 1999 SSL обеспечивал защищенное соединение, которое могут использовать протоколы более высокого уровня – HTTP, FTP, SMTP и т. д. Наиболее широко он используется для защиты данных передаваемых по HTTP (режим HTTPS). Для этого должны использоваться SSL-совместимые web-сервер и браузер.

С точки зрения выполняемых действий, различия между этими протоколами SSL и TLS весьма невелики, но в то же время, они несовместимы друг с другом [7,8].

Протокол предусматривает два этапа взаимодействия клиента и сервера:

1) установление SSL-сессии (процедура «рукопожатия», от англ. «handshake»): на этом этапе может производиться аутентификация сторон соединения, распределение ключей сессии, определяются настраиваемые параметры соединения;

2) защищенное взаимодействие.

Протоколом SSL используются следующие криптоалгоритмы:

- асимметричные алгоритмы RSA и Диффи-Хеллмана;
- алгоритмы вычисления хэш-функций MD5 и SHA1;
- алгоритмы симметричного шифрования RC2,RC4, DES, TripleDES, IDEA.

На смену SSL v3.0 пришел протокол TLS v1.0 (Transport Layer Security) - последняя версия TLS.

Протокол SSL позволяет проводить следующие варианты аутентификации сторон взаимодействия:

- аутентификация сервера без аутентификации клиента (односторонняя аутентификация) – это наиболее часто используемый режим, позволяющий установить подлинность сервера, но не проводящий проверки клиента (ведь подобная проверка требует и от клиента наличия сертификата);
- взаимная аутентификация сторон (проверяется подлинность как клиента, так и сервера);
- отказ от аутентификации – полная анонимность; в данном случае SSL обеспечивает шифрование канала и проверку целостности, но не может защитить от атаки путем подмены участников взаимодействия.

## 3.3. Протоколы IPSec и распределение ключей

Протокол IPSec или, если точнее, набор протоколов, является дополнением к использующемуся сейчас протоколу IP ver.4 и составной частью IP ver.6. Возможности, предоставляемые протоколами IPSec:

- контроль доступа;
- контроль целостности данных;
- аутентификация данных;
- защита от повторений;
- обеспечение конфиденциальности.

Основная задача IPSec – создание между двумя компьютерами, связанными через общедоступную (небезопасную) IP-сеть, безопасного туннеля (рис. 3.2), по которому передаются конфиденциальные или чувствительные к несанкционированному изменению данные. Подобный туннель создается с использованием криптографических методов защиты информации. Протокол работает на сетевом уровне модели OSI и, соответственно, он «прозрачен» для приложений. Иными словами, на работу приложений (таких как web-сервер, браузер, СУБД и т. д.) не влияет, используется ли защита передаваемых данных с помощью IPSec или нет.

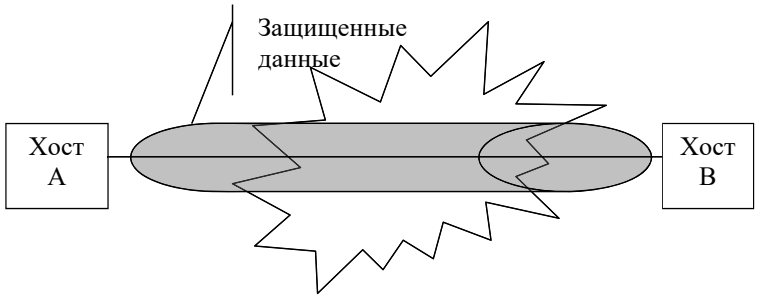


Рис. 3.2. Туннель безопасности

Архитектура IPSec является открытой, что позволяет использовать для защиты передаваемых данных новые криптографические алгоритмы, например, алгоритмы, соответствующие национальным стандартам. Для этого необходимо, чтобы взаимодействующие стороны поддерживали эти алгоритмы, и они были бы стандартным образом зарегистрированы в описании параметров соединения.

Процесс защищенной передачи данных регулируется правилами безопасности, принятыми в системе. Параметры создаваемого туннеля описывает информационная структура, называемая контекст защиты или ассоциация безопасности («Security Association», сокр. SA). Как уже отмечалось выше, IPSec является набором протоколов, и состав контекста защиты может различаться. В зависимости от конкретного протокола в него входит:

- IP-адрес получателя;
- указание на протоколы безопасности, используемые при передаче данных;
- ключи, необходимые для шифрования и формирования имитовставки (если это требуется);
- указание на метод форматирования, определяющий, каким образом создаются заголовки;
- индекс параметров защиты (от англ. «Security Parameter Index», сокр. SPI) – идентификатор, позволяющий найти нужный SA.

Обычно, контекст защиты является однонаправленным, а для передачи данных по туннелю в обе стороны задействуются два SA. Каждый хост имеет свою базу контекстов защиты, из которой выбирается нужный элемент либо на основании значения SPI, либо по IP- адресу получателя.

Два протокола, входящие в состав IPSec, это:

1) протокол аутентифицирующего заголовка – AH («Authentication Header»), обеспечивающий проверку целостности и аутентификацию передаваемых данных;

2) протокол инкапсулирующей защиты данных – ESP («Encapsulating Security Payload»), обеспечивающий конфиденциальность и, опционально, проверку целостности и аутентификацию.

Оба эти протокола имеют два режима работы – транспортный и туннельный, последний определен в качестве основного. Туннельный режим используется, если хотя бы один из соединяющихся узлов является шлюзом безопасности. В этом случае создается новый IP- заголовок, а исходный IP-пакет полностью инкапсулируется в новый.

Транспортный режим ориентирован на соединение хост-хост. При использовании ESP в транспортном режиме защищаются только данные IP-пакета, заголовок не затрагивается. При использовании AH защита распространяется на данные и часть полей заголовка.

## 3.4. Межсетевые экраны

***Межсетевой экран (МЭ)*** – это средство защиты информации, осуществляющее анализ и фильтрацию проходящих через него сетевых пакетов. В зависимости от установленных правил МЭ пропускает или уничтожает пакеты, разрешая или запрещая таким образом сетевые соединения.

МЭ является классическим средством защиты периметра компьютерной сети: он устанавливается на границе между внутренней (защищаемой) и внешней (потенциально опасной) сетями и контролирует соединения между узлами этих сетей.

Как уже было отмечено, фильтрация производится на основании правил. Наиболее безопасным при формировании правил для МЭ считается подход «запрещено все, что явно не разрешено». В этом случае сетевой пакет проверяется на соответствие разрешающим правилам, а если таковых не найдется – отбрасывается. Но в некоторых случаях применяется и обратный принцип: «разрешено все, что явно не запрещено». Тогда проверка производится на соответствие запрещающим правилам и, если таких не будет найдено, пакет будет пропущен.

Фильтрацию можно производить на разных уровнях эталонной модели сетевого взаимодействия OSI. По этому признаку МЭ делятся на следующие классы [6-8]:

- экранирующий маршрутизатор;
- экранирующий транспорт (шлюз сеансового уровня);
- экранирующий шлюз (шлюз прикладного уровня).

Экранирующий маршрутизатор (или пакетный фильтр) функционирует на сетевом уровне модели OSI, но для выполнения проверок может использовать информацию и из заголовков протоколов транспортного уровня. Соответственно, фильтрация может производиться по ip-адресам отправителя и получателя, а также по TCP и UDP портам. Такие МЭ отличает высокая производительность и относительная простота – функциональностью пакетных фильтров сейчас обладают даже наиболее простые и недорогие аппаратные маршрутизаторы. В то же время, они не защищают от многих атак, например, связанных с подменой участников соединений.

Шлюз сеансового уровня работает на сеансовом уровне модели OSI и также может контролировать информацию сетевого и транспортного уровней. Соответственно, в дополнение к перечисленным выше возможностям, подобный МЭ может контролировать процесс установки соединения и проводить проверку проходящих пакетов на принадлежность разрешенным соединениям.

Шлюз прикладного уровня может анализировать пакеты на всех уровнях модели OSI от сетевого до прикладного, что обеспечивает наиболее высокий уровень защиты. В дополнение к ранее перечисленным, появляются такие возможности, как аутентификация пользователей, анализ команд протоколов прикладного уровня, проверка передаваемых данных (на наличие компьютерных вирусов, соответствие политике безопасности).

В последнее время стал широко использоваться вариант установки программного МЭ непосредственно на защищаемый компьютер. Иногда такой МЭ называют «персональным». Подобная схема позволяет защититься от угроз исходящих не только из внешней сети, но из внутренней.

## 4. Защита локальной беспроводной сети стандарта IEEE 802.11

Набор стандартов IEEE (Institute of Electrical and Electronics Engineers) 802.11 является основой для беспроводной связи в ограниченной области (локальной сети). 802.11 является первым отраслевым стандартом для беспроводных локальных сетей WLAN [10]. Стандарт разработал IEEE в 1997 году. Наибольшую популярность получили беспроводные сети стандарта IEEE 802,11b/g/n, IEEE 802.11ac и IEEE 802.11ax.

Стандарты IEEE 802.11 используют соединение по радиоканалам на следующих частотах:

- 2,4 ГГц (полоса частот 2400...2483,5 МГц);
- 5 ГГц (диапазон частот 5,180...5,240 ГГц и 5,745...5,825 ГГц).

Безопасная передача данных по сетям стандарта 802.11 обеспечивается рядом технологий и протоколов, таких как WEP, WPA, WPA2 и WPA3, которые управляют аутентификацией пользователей, шифрованием и обеспечением целостности сетевого трафика.

***Протоколы безопасности беспроводной связи, такие как Wired Equivalent Privacy (WEP) и Wi-Fi Protected Access (WPA),*** — это протоколы безопасности аутентификации, созданные Wireless Alliance, используемые для обеспечения безопасности беспроводной сети.

В настоящее время доступно четыре протокола беспроводной безопасности:

- WEP;
- WPA;
- WPA 2;
- WPA 3.

Первые два из них являются устаревшими, и производители программного и аппаратного обеспечения отказываются от их поддержки.

Wired Equivalent Privacy (WEP) — это первый протокол безопасности, когда-либо применявшийся на практике. Разработанный в 1997 году, он устарел, но до сих пор используется в наше время со старыми устройствами.

WEP использует схему шифрования данных, основанную на сочетании значений ключей, генерируемых пользователем и системой. Тем не менее, широко известно, что WEP является наименее безопасным типом сети, поскольку хакеры разработали тактику обратного инженерии и взлома системы шифрования.

Защищенный доступ Wi-Fi (WPA) был разработан для борьбы с недостатками, обнаруженными с протоколом WEP. WPA предлагает такие функции, как протокол целостности временного ключа (TKIP). TKIP был динамическим 128-битным ключом, который было труднее взломать, чем статический, неизменный ключ WEP.

Он также представил проверку целостности сообщений, которая сканировала любые измененные пакеты, отправленные хакерами, TKIP и предварительный ключ (PSK), среди прочего, для шифрования.

В 2004 году WPA2 внес значительные изменения и больше функций в беспроводной гамбит безопасности. WPA2 заменил TKIP протоколом кода аутентификации сообщений Counter Mode Cipher Block Chaining (CCMP), который является гораздо превосходным инструментом шифрования.

WPA2 является отраслевым стандартом с момента его создания. 13 марта 2006 года Wi-Fi Alliance заявил, что все будущие устройства с торговой маркой Wi-Fi должны использовать WPA2.

Стандарт WPA2 исправлял уязвимости, обнаруженные в стандарте WEP. В конце 2004 года основные проблемы безопасности сетей стандарта 802.11 были решены. В 2006 году WPA2 начал активно внедряться во все виды оборудования и стал главным требованием для всех устройств с поддержкой Wi-Fi.

Набор стандартов IEEE 802.11 рассматривает четыре варианта аутентификации:

- аутентификация для систем с открытым ключом (Open Authentication);
- аутентификация с общим ключом (Shared Key Authentication);
- WPA2-PSK с предустановленным ключом;
- WPA2-Enterprise с аутентификацией на RADIUS-сервере.

WPA2-PSK требует одного пароля для подключения к беспроводной сети. Общепринято, что один пароль для доступа к Wi-Fi безопасен, но только настолько, насколько вы доверяете тем, кто его использует. Серьезная уязвимость возникает из-за потенциального повреждения, нанесенного при

попадании учетных данных в систему не в те руки. Вот почему этот протокол чаще всего используется для сети в жилых домах или открытой сети Wi-Fi.

WPA2-Enterprise требует RADIUS-сервера, который обрабатывает задачу аутентификации доступа пользователя сети. Фактический процесс аутентификации основан на политике 802.1X и поставляется в нескольких различных системах с маркировкой EAP (рис. 4.1).

Поскольку каждое устройство аутентифицируется перед подключением, между устройством и сетью эффективно создается персональный зашифрованный туннель. Преимущества безопасности правильно настроенного WPA2-Enterprise обеспечивают почти непроходимую сеть.

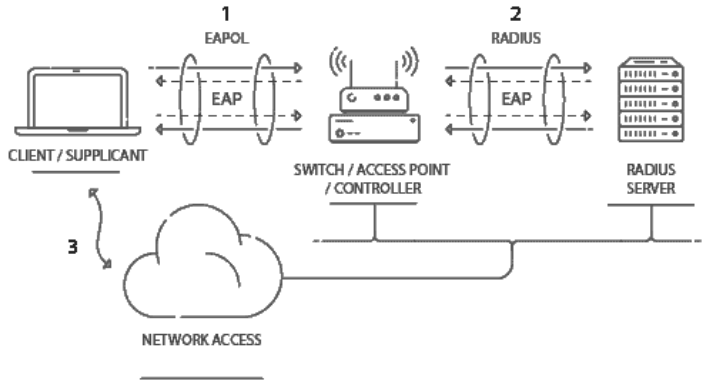


Рис. 4.1. Обмен данными в сети Wi-Fi

Есть всего несколько компонентов, которые необходимы для работы WPA2-Enterprise. На практике, если у вас уже есть точки доступа и свободное серверное пространство, то вы обладаете всем оборудованием, необходимым для этого.

Чтобы зашифровать сеть с помощью WPA2-PSK, нужно предоставить маршрутизатору не ключ шифрования, а просто латинскую парольную фразу длиной от 8 до 63 символов. Используя CCMP, эта парольная фраза вместе с SSID сети используется для генерации уникальных, постоянно изменяющихся ключей шифрования для каждого беспроводного клиента. Хотя WEP также поддерживает парольные фразы, для него это только способ более легко создавать статические ключи, которые обычно состоят из шестнадцатеричных символов 0-9 и A-F.

Набор технологий WPA3 имеет следующие преимущества:

- WPA3 благодаря индивидуальному шифрованию сетевых пакетов повышает конфиденциальность передаваемых пользователями данных в открытых сетях;

- встроены механизмы защиты от атаки методом полного перебора;

- внедрена облегченная настройка для устройств Интернета вещей (IoT), с помощью которой пользователь имеет возможность, благодаря телефону или планшету, настроить параметры Wi-Fi WPA3 на устройствах без экрана;

- внедрен модернизированный криптографический стандарт для сетей Wi-Fi, так называемый 192-разрядный пакет безопасности.

Поскольку сети Wi-Fi различаются по целям использования и требованиям безопасности, то WPA3, как и WPA2, включает два профиля:

- WPA3-Personal;

- WPA3-Enterprise.

Для повышения эффективности обновлений PSK для WPA3-PSK предлагают большую защиту за счет улучшения процесса аутентификации.

Стратегия для этого использует одновременную аутентификацию равных (SAE). Этот протокол требует взаимодействия пользователя при каждой попытке аутентификации, что приводит к значительному замедлению для тех, кто пытается грубо выполнить процесс аутентификации.

WPA3-Enterprise предлагает некоторые дополнительные преимущества, но это в целом небольшие изменения с точки зрения безопасности с переходом от WPA2-Enterprise.

Значительное улучшение, которое предлагает WPA3-Enterprise, заключается в том, чтобы проверка сертификата сервера была настроена для подтверждения подлинности сервера, к которому подключается устройство. Однако из-за отсутствия серьезных улучшений вряд ли это будет быстрый переход на WPA3.

Пользователи WPA3 Personal получают надежную защиту от попыток подбора пароля, в то время как пользователи WPA3-Enterprise теперь могут использовать протоколы безопасности более высокого уровня.

Таким образом, технология WPA3 является более совершенной, надежной и удобной в использовании. Разработка WPA3 — это большой шаг на пути к совершенствованию безопасности беспроводных сетей.

Внедрение технологии WPA3 в массы будет происходить в течение нескольких ближайших лет. Причина этого заключается в том, что сертификация устройств для WPA3 пока что не обязательна по правилам WiFi Alliance, а происходит по желанию производителей.

## 5. Защита баз данных

***База данных (БД)*** — это имеющая название совокупность данных, которая отражает состояние объектов и их отношений в рассматриваемой предметной области.

***Система управления базами данных (СУБД)*** — это программное обеспечение, которое необходимо для создания, редактирования и обслуживания файлов БД.

В БД чаще всего используется язык структурированных запросов SQL, созданный для того, чтобы получать необходимую информацию из базы данных.

Структура типовой базы данных представлена на рисунке 5.1.

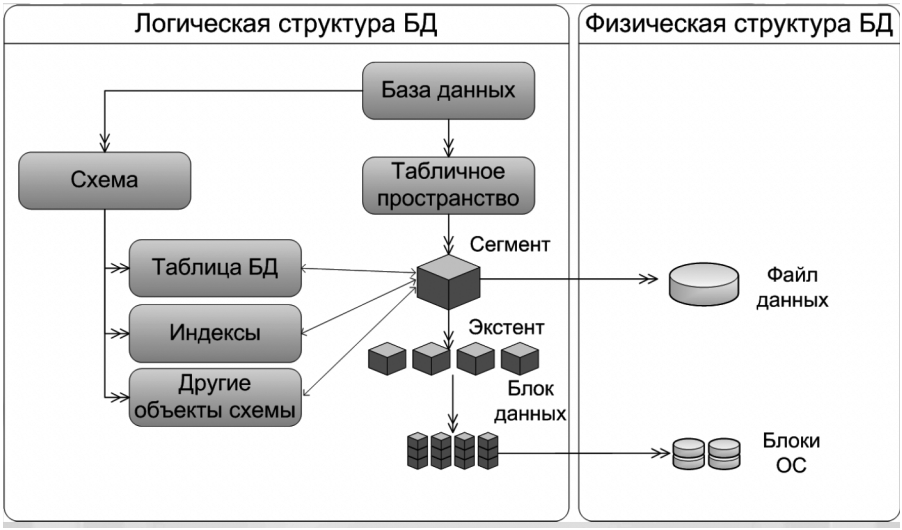


Рис. 5.1. Структура типовой БД

Уровни представления данных [10]:

- «физический» уровень;
- уровень операционной системы и специализированного программного обеспечения;
- «логический уровень» (уровень СУБД);
- уровень представления информации.

Существуют следующие уровни угроз безопасности баз данных:

- угрозы конфиденциальности данных;
- угрозы целостности данных;
- угрозы доступности данных;
- общие угрозы безопасности информационных систем;
- специфические угрозы безопасности БД.

Уязвимые места уровней безопасности баз данных:

1. Прослушивание, перехват и модификация данных.
2. Фальсификация пользователей:
   - угрозы при использовании парольной защиты;
   - «человеческий фактор».
3. Неавторизированный доступ к таблицам, столбцам или строкам данных:
   - SQL – инъекции;
4. Проблемы подотчетности.
5. Сложность администрирования доступа к данным.
6. Блокирование данных:
   - «зловредное» использование ограничений;
   - потерянные измерения.

***SQL-инъекция*** или SQLi – уязвимость, которая позволяет атакующему использовать фрагмент вредоносного кода на языке структурированных запросов (SQL) для манипулирования базой данных и получения доступа к потенциально ценной информации.

Атаки на основе этого вида уязвимости могут использоваться для следующих целей:

- получение доступа к данным, которые обычно недоступны, или к данным конфигурации системы, которые могут использоваться для дальнейших атак;
- получение несанкционированного доступа к ресурсам локальной вычислительной сети через сервер, на котором развернута БД;
- выполнение произвольного кода в системе, на которой расположена СУБД с правами функционирующего сервера.

Рассмотрим механизмы защиты баз данных.

Принцип минимальных привилегий:

- сформировать минимальную конфигурацию ПО и запущенных сервисов СУБД;
- предоставить доступ к ОС и базе данных только уполномоченным пользователям;
- ограничить доступ к административным аккаунтам ОС;
- ограничить доступ к административным аккаунтам СУБД:
- ограничить доступ пользователей только к тем объектам БД, которые им нужны для работы.

Механизмы обеспечения целостности на физическом уровне:
- физическая защита;
- дублирование или защита носителей;
- резервное копирование данных (средствами ОС и СУБД).

Механизмы обеспечения целостности средствами СУБД:
- декларативные средства контроля целостности;
- транзакции и блокирование;
- триггеры (процедурные средства контроля целостности);
- средствами имитозащиты (при передаче по сети).

***Транзакция*** – это последовательность операторов манипулирования данными, выполняющаяся как единое целое и переводящая базу данных из одного целостного состояния в другое целостное состояние.

Транзакции обладают следующими свойствами:
- атомарность;
- согласованность;
- изоляция;
- долговечность.

Механизмы обеспечения конфиденциальности:
- разграничение доступа;
- криптографические методы защиты;
- аудит.

Механизмы обеспечения высокой доступности:
- физическая защита, дублирование носителей;
- настройка производительности и оптимизация;
- управление транзакциями и блокировками;
- архивирование данных (управление задачами резервного копирования и восстановления).

Активное сопровождение БД состоит из сбора статистики и анализа сигнальных сообщений, реагирование на сигналы. Управление производительностью состоит из мониторинга, настройки кода SQL, планов доступа к данным и индексирования.

Чтобы БД работала без сбоев необходимо включить режим архивирования, мультиплексировать управляющие, журнальные и архивные файлы на нескольких дисках и контроллерах, а также планировать резервирование и надежно хранить резервные копии.

# Раздел 2. ЗАЩИТНЫЕ МЕХАНИЗМЫ ИСПОЛЬЗУЕМЫЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

## 6. Системы обнаружения вторжений

***Система обнаружения вторжений (СОВ)*** – множество различных программных и аппаратных средств, объединяемых одной общей задачей – они занимаются анализом использования вверенных им ресурсов и, в случае обнаружения каких-либо подозрительных или просто нетипичных событий, способны предпринимать некоторые самостоятельные действия по обнаружению, идентификации и устранению их причин [10].

К основным функциям СОВ относятся:

- выявление вторжений и сетевых атак;
- запись всех событий;
- поиск уязвимостей;
- прогнозирование атак;
- распознавание источника атаки: инсайд или взлом;
- информирование служб ИБ об инциденте в реальном времени;
- формирование отчетов.

Один из вариантов архитектуры СОВ представлен на рисунке 6.1.

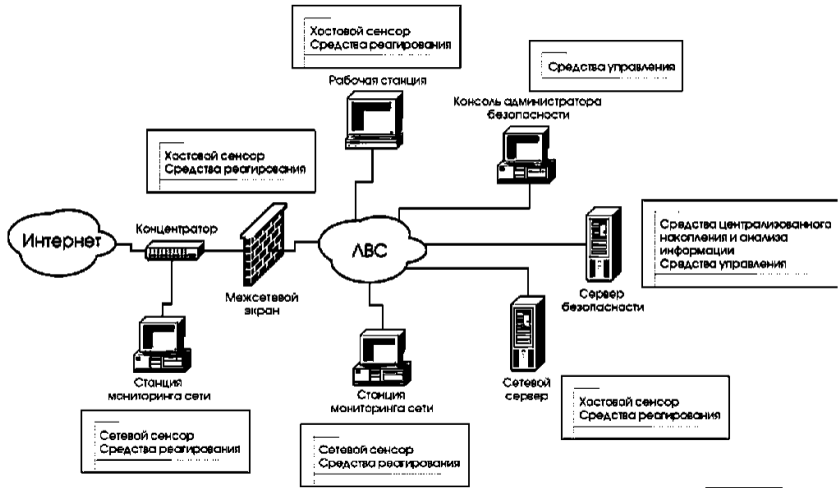


Рис. 6.1. Типовая архитектура СОВ

Типовая система обнаружения вторжений, чаще всего, состоит из:

- сенсорной подсистемы;
- подсистемы анализа;
- хранилища;
- подсистемы реагирования на выявленные вторжения;
- консоли управления.

Система обнаружения вторжений собирает и анализирует полученные данные, хранит события с момента подключения к сетевой инфраструктуре и формирует отчеты и управляется из консоли администратора.

Системы обнаружения вторжений можно классифицировать по источнику информации, по методу анализа, по реакции на выявленное вторжение и по режиму работы.

По источнику информации СОВ классифицируются:

- сетевые;
- хостовые;
- протокольные;
- гибридные;
- уровня приложений.

По методу анализа СОВ делятся на обнаружение злоупотреблений и на обнаружение аномалий.

По реакции на выявленное вторжение - выделяют активные и пассивные.

Системы обнаружения вторжений имеют два режима работы, такие как непрерывный мониторинг и периодические запуски.

Рассмотрим чаще всего используемые варианты реализации СОВ, их достоинства и недостатки.

Преимущества сетевых СОВ:

- несколько оптимально расположенных СОВ могут контролировать большую сеть;
- развертывание сетевых СОВ не оказывает большого влияния на производительность сети;
- сетевые СОВ практически неуязвимыми для атак.

Недостатки:

- не в состоянии распознавать нападение, начатое в момент высокой загрузки сети;
- дополнительные сложности при анализе сетей, построенных на коммутаторах;
- не могут анализировать зашифрованную информацию;
- не могут определить, была ли успешна предпринятая атака;

- проблемы с определением сетевых атак, которые включают фрагментированные пакеты.

Достоинства хостовых СОВ:

- обнаруживают нападения, которые не выявляют СОВ, защищающие сегмент сети;

- способны анализировать данные, до того, как они будут зашифрованы на сервере до их отправки потребителю;

- на функционирование хостовых СОВ не влияет наличие в сети коммутаторов;

- при работе хостовых СОВ с результатами аудита операционных систем (ОС), они могут оказать помощь в определении троянских программ или других атак, которые нарушают целостность ПО.

Недостатки хостовых СОВ:

- должны устанавливаться и поддерживаться на каждом хосте, который будет контролироваться;

- могут сами являться объектом атаки;

- часто не имеют возможности выявить исследования, при которых целью является вся сеть;

- испытывают трудности в обнаружении и противодействии нападениям с отказом в обслуживании;

- используют вычислительные ресурсы хоста, который контролируют.

Преимущества СОВ уровня приложения:

- контролируют деятельность с очень высокой степенью детализации;

- могут работать в средах, использующих шифрование.

Недостатки;

- более уязвимы, чем хостовые СОВ;

- просматривают события на пользовательском уровне абстракции;

- не для всех видов приложений существуют подходящие СОВ.

Таким образом, использование СОВ помогает достичь нескольких целей:

- обнаружить вторжение или сетевую атаку;

- спрогнозировать возможные будущие атаки и выявить уязвимости для предотвращения их дальнейшего развития;

- выполнить документирование существующих угроз;

- обеспечить контроль качества администрирования с точки зрения безопасности, особенно в больших и сложных сетях;

- определить расположение источника атаки по отношению к локальной сети (внешние или внутренние атаки), что важно при принятии решений о расположении ресурсов в сети.

## 7. Системы защиты внутреннего информационного периметра

Типовым примером системы защиты внутреннего информационного периметра является DLP – система [10].

***DLP-система (Data Leak Prevention***) — это специализированное ПО, которое защищает организацию от утечек данных. Данная технология – это не только возможность блокировать передачу конфиденциальной информации по различным каналам, но и инструмент для наблюдения за ежедневной работой сотрудников, который позволяет найти слабые места в безопасности до наступления инцидента.

Часто в компаниях больше внимание уделяют внешним угрозам: спаму и фишинг-атакам типа «отказ в обслуживании», вирусам (троянскому ПО, червям), подмене главных страниц интернет-ресурсов, шпионскому и рекламному программному обеспечению, социальному инжинирингу. Но на самом деле внутренние угрозы способны причинить компании более серьезный ущерб, чем злоумышленники за ее пределами.

В принципе, любой работник компании может являться потенциальным инсайдером и поставить информационную безопасность под угрозу. От злого умысла или банальной оплошности не застрахован никто: от низшего звена и до руководства.

Принцип работы DLP-системы прост и заключается в анализе всей информации: исходящей, входящей и циркулирующей внутри компании. Система при помощи алгоритмов анализирует, что это за информация, и в случае, если она критичная и отправляется стороннему адресату — блокирует передачу и/или уведомляет об этом ответственного сотрудника.

Основа DLP — набор правил. Они могут быть любой сложности и касаться разных аспектов работы. Если кто-то их нарушает, то ответственные лица получают об этом уведомление.

Система отслеживает не только время работы и активные программы на компьютере, но и любую другую работу с информацией, — ввод данных с клавиатуры, переписку и передачу файлов по почте, в соцсетях и мессенджерах, отправляемые на печать документы, время простоя, SIP-телефонию, активность на сайтах и многое другое.

*Способы перехвата данных*

Для того, чтобы анализировать данные — DLP-система сперва должна их получить.

Есть два основных способа перехвата — ***серверный и агентский.***

В первом случае, система контролирует сетевой трафик на сервере, через который компьютеры «общаются» с внешним миром.

Во втором случае, специальные небольшие программы — агенты — устанавливаются на все компьютеры организации и передают с каждой машины данные для анализа.

Агентский перехват является более распространённым, ведь с его помощью можно получить гораздо больше данных из различных каналов коммуникации, а значит и надежнее предотвратить возможные утечки.

В настоящее время существуют разные по своей функциональности DLP-системы:

l. Полноценные DLP с большими возможностями контроля и блокировки передачи информации и анализа данных;

2. Системы с частичным функционалом DLP, которые могут отследить перемещение данных, но не могут предотвратить утечку;

3. Системы другого класса со встроенным модулем DLP.

Разные системы решают различный спектр задач. Для того чтобы разобраться в этом, важно понимать, как они эволюционировали.

*Эволюция DLP*

Изначально DLP-рынок возник из проблемы выполнение требований законодательства, в частности с того момента, когда регуляторы обратили внимание на утечки информации в компаниях и разработали ряд законов и отраслевых стандартов относительно защиты информации от внутренних угроз, которых нужно было каким-то образом придерживаться. Для решения задачи информационной безопасности разработали специальный инструмент – DLP-систему.

Второй этап разработки – DLP для защиты коммерческой тайны. Если раньше системой пользовались организации, в основном оперирующие персональными и финансовыми данными клиентов, то в дальнейшем у этих же организаций возник спрос на защиту собственной коммерческой информации. Это дало толчок для пересмотра концепции DLP и ее переформатирования в более сложную систему для максимального контроля каналов передачи данных.

Следующим шагом стала DLP для внутренней безопасности, то есть система уже не только предотвращала утечку информации, но и позволяла детально анализировать информацию и выявлять инциденты. Возможности такой DLP отчасти пополнились функционалом других классов ИБ-систем, таких как платформы для расследования инцидентов. Данный класс DLP начал формироваться относительно недавно.

*Новое поколение DLP – борьба с корпоративными мошенниками*

После того, как полноценные DLP созрели в своих аналитических возможностях по выявлению инцидентов, разработчики обратили внимание на применение системы для борьбы с мошенничеством в компаниях, в том числе с

экономическими нарушениями. Архив большого количества информации о пользователях, собранной DLP-решением, анализ действий сотрудников и предоставление специалистам службы информационной безопасности максимального количества инструментов – одни из основных векторов развития DLP систем.

Какими характеристиками должна обладать современная DLP-система?

*Полный архив файлов, событий, инцидентов.*

Во-первых, такие системы ведут полный архив передаваемых и найденных файлов, событий и инцидентов, в отличие от предыдущих поколений DLP, которые фиксировали только случаи несоблюдения политик безопасности.

Благодаря возможностям системы фиксировать и сохранять такую детальную информацию департамент безопасности может видеть как общую картину состояния защищенности предприятия, так и детально расследовать инциденты внутренней безопасности вплоть до составления досье на сотрудника и его круг общения.

*Управление и расследование.*

Удобство управления и широкие возможности по расследованию инцидентов – одни из важнейших показателей современной DLP-системы. Речь идет о наличии единого для всех компонентов DLP веб-интерфейса с возможностью построения различных отчетов, начиная от досье сотрудников со списком их взаимодействий с другими пользователями и заканчивая специальным отчетом для топ-менеджеров компании.

*Поведенческий анализ.*

Новый уровень DLP-систем представляет собой совокупность основных возможностей перехвата и блокировки передачи данных и функционала других классов ИБ-решений, например поведенческого анализа пользователей или UBA (User Behavior Analytics). DLP-разработчики обратили внимание на данный класс решений, позволяющих выявлять стандартное поведение работников, а в случае отклонения от этих норм – принимать меры, к примеру уделять больше внимания подозрительным сотрудникам.

Разработчики DLP пришли к выводу, что такой функционал будет отличным дополнением к системе, которая находится в стадии трансформации в ИБ-решение тотального контроля пользователей.

*Контроль эмоционального состояния.*

Помимо анализа поведения сотрудников, можно оценивать уровень их эмоционального состояния. Система анализирует и оценивает всю лексику исходящих сообщений пользователя в мессенджерах, электронной почте и соцсетях. Анализ проводится на основе специального встроенного словаря

тональной лексики, который состоит из "эмоциональных" слов, часто используемых человеком, в том числе в разговорной речи.

В свою очередь, список структурируется по определенным типам эмоций: радость, доверие, ожидание, грусть, недовольство, страх, удивление, злость. Анализ динамики эмоционального состояния позволяет выделять тех сотрудников, кто может попасть в группу риска. Таких можно также взять на особый контроль.

*Архитектура решения.*

Споры о том, что лучше – агентская DLP-система или шлюзовая, ведутся давно. Каждый из вариантов имеет не только преимущества, но и недостатки.

Компенсировать их позволяет смешанная архитектура с компонентами контроля информационных потоков на почтовом и сетевом шлюзах, рабочих станциях, модулем для выявления мест хранения конфиденциальной информации и общими сервисами, такими как архив, рисунок 7.1.

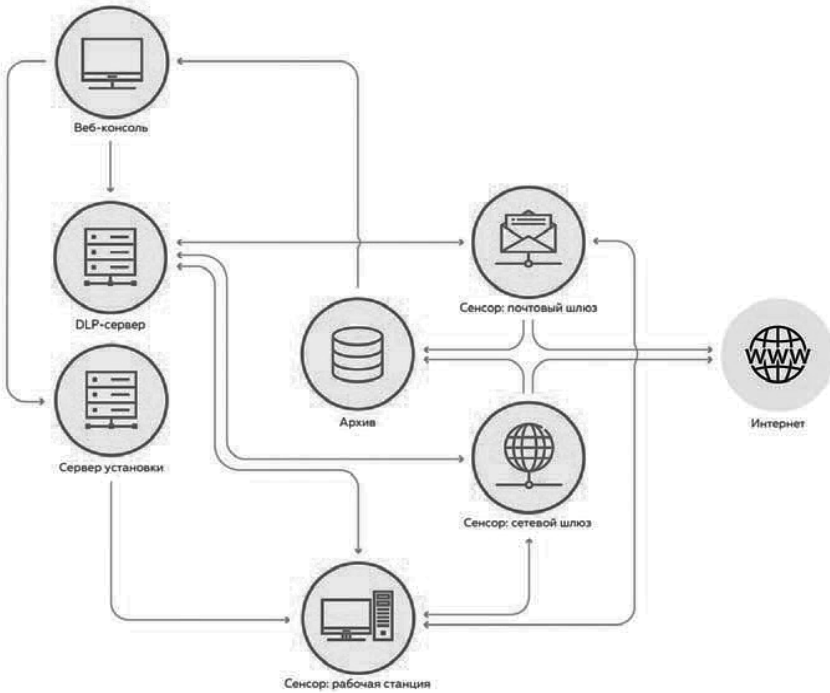


Рис. 7.1. Смешанная архитектура DLP – системы

Поскольку внутренние сети многих компаний устроены по-разному, а бизнес-процессы существенно различаются, для современной DLP важно быть гибкой в плане установки и интеграции. Этому способствуют модульность и наличие компонентов для контроля на разных участках сети.

*Криптопериметр.*

Иными словами, это контентно-зависимое шифрование. DLP может принудительно шифровать файлы при копировании их на съемные устройства в зависимости от настроенных политик безопасности. Такой функционал позволяет избегать популярного сценария утечки, когда сотрудники теряют флешки с конфиденциальными данными, а также в случае кражи или использования устройства третьими лицами. Криптопериметр – уникальная функция для DLP-систем.

*Расширенные возможности мониторинга действий.*

Сбор большого объема информации о пользователях, анализ действий сотрудников и предоставление специалистам службы безопасности максимального количества данных о пользователях – ключевые направления развития DLP в ближайшие годы. Поэтому расширенные возможности мониторинга действий сотрудников – еще один показатель современной DLP-системы. Сюда входят достаточно простые методы контроля за действиями, но при необходимости они могут сильно помочь в расследовании серьезного инцидента.

К таким методам относятся отслеживание нажатий клавиатуры (кейлогер), запись звуков через микрофон контролируемого компьютера, создание снимков с фронтальной веб-камеры.

*Camera Detector.*

Это уникальная в своем роде технология с функцией защиты от фотографирования экрана компьютера. Встроенная технология определяет устройство, сообщает об этом специалисту по информационной безопасности и сохраняет инцидент в архиве с информацией о том, на каком компьютере и в какое время это было сделано.

Такой инструмент востребован в первую очередь среди финансовых организаций и компаний, работающих с большими объемами персональных данных, которые могут быть украдены третьими лицами.

*Создание единой платформы защиты.*

Базовые технологии DLP давно доведены до совершенства, и сейчас разработчики сосредоточились на повышении удобства использования системы и возможности полноценного расследования инцидентов. При этом развитие систем диктуется не только требованиями заказчиков, но и появлением новых

инсайдерских угроз, в числе которых находится специфическое фотографирование монитора на смартфон.

Можно с уверенностью говорить, что сегодня основным вектором развития DLP является возможность эффективного предотвращения злоупотреблений. Достигается это путем развития единой платформы для аналитической работы, полноценного расследования инцидентов и защиты не только конфиденциальных данных, но и финансовых средств компании.

## 8. Центр обеспечения информационной безопасности

***Центр обеспечения информационной безопасности, SOC – (Security Operations Center***) — это структурное подразделение, осуществляющее мониторинг работы систем защиты информации и реагирующее на инциденты информационной безопасности. Также это специалисты по защите информации, которые непрерывно осуществляют контроль за сообщениями, поступающими от технических средств, для того, чтобы как можно оперативнее устранить угрозу информационной безопасности.

Итак, Центр SOC - это не только технические системы, в режиме реального времени передающие аналитикам SOC сообщения от средств защиты, но и сами люди - эксперты, которые могут отличить ложное срабатывание защитного средства от настоящего, «боевого», и способные понять, являются ли несколько явно не связанных между собой сообщений от средств защиты звеньями одной цепи, означающей компьютерное заражение.

Для успешной работы SOC большое значение имеют дополнительные системы: SIEM (Security Information and Event Management — системы управления информацией о безопасности и событиями информационной безопасности), IRP (Incident Response Platform — платформы реагирования на инциденты информационной безопасности), SOAR (Security Orchestration, Automation and Response - системы управления, автоматизации и реагирования на инциденты), SGRC (Security Governance, Risk-management and Compliance — системы управления информационной безопасностью, рисками и соответствием законодательству).

***Основная задача SOC-Центра*** — это обеспечение реагирования на инциденты информационной безопасности в рамках заранее согласованных SLA (Service Level Agreement - соглашение о качестве оказываемых услуг). Предварительно также обговариваются задаваемые критерии KPI (Key Performance Indicators - ключевые показатели эффективности) для команд реагирования SOC-Центров и определенные типы шагов по реагированию на кибератаки, их сдерживанию, локализации и нейтрализации угроз

информационной безопасности, которые будут предприниматься командой SOC в рамках обработки инцидентов ИБ.

SOC-Центры могут быть ***внутренними*** и ***внешними***.

*Внутренний SOC*, как правило, создается после того, как руководитель крупной компании, проведя анализ рисков и осознав наличие актуальных угроз в области информационной безопасности, принимает решение о том, что необходимо оперативно, а лучше круглосуточно, то есть в режиме 24/7, реагировать на возникающие инциденты информационной безопасности. При этом, как правило, имеющихся ресурсов ИБ или ИТ-департаментов для круглосуточного дежурства не хватает, поэтому создается внутренний SOC-Центр, в который набирают самых опытных штатных сотрудников компании и нанимают новых экспертов по ИБ.

*Внешний же Центр SOC* — это, по сути, аутсорсинговая услуга по оперативному реагированию на инциденты информационной безопасности, когда компания-заказчик заключает договор на обслуживание с внешним Центром SOC. При этом дополнительных сотрудников в штат компании не набирают, а целиком и полностью полагаются на специалистов внешнего SOC-Центра, которые, в соответствии с оговоренными SLA и KPI, выполняют работу по реагированию на кибератаки, выявлению и расследованию инцидентов информационной безопасности. В этом случае компания-заказчик экономит на штатных сотрудниках и получает прогнозируемое, согласованное в договоре время реагирования со стороны высококлассных специалистов из внешнего SOC.

***Алгоритм подключения и использования*** услуг SOC-Центра выглядит следующим образом:

1. Заказчик услуг SOC-Центра, который видит необходимость в аутсорсинге оперативного реагирования на свои инциденты ИБ, обращается к менеджерам SOC с запросом о подключении к сервисам SOC.

2. Менеджеры Центра SOC согласовывают детали подключения информационных и защитных систем заказчика к инфраструктуре SOC-Центра для того, чтобы оперативно обрабатывать поступающие данные без выезда на площадку Заказчика.

3. Инженеры внешнего SOC-Центра подключают источники информации и событий ИБ компании-заказчика в свою внутреннюю систему управления инцидентами. При этом следует обеспечить надежный и защищенный канал связи между компанией-заказчиком и внешним SOC-Центром для обеспечения оперативного обмена информацией.

4. На площадке заказчика информационные системы и имеющиеся средства технической защиты настраиваются на пересылку всей значимой с точки зрения ИБ информации во внешний SOC.

5. Во внешнем SOC-Центре входящие данные непрерывно обрабатываются сотрудниками SOC (дежурной сменой), которая состоит, как правило, ***из следующих специалистов***:

- *системный администратор или инженер* - тот, кто настраивает внутренние системы SOC-Центра, которые используются в обработке инцидентов заказчиков, а также отвечает за стабильность получения данных из систем компании-заказчика. Такому специалисту просто необходимо быть “на ты” с различными типами операционных систем, прикладным ПО, разнообразными системами киберзащиты. В случае, если в коммерческом SOC-Центре используется какое-то самостоятельно созданное программное обеспечение, то на системного администратора SOC могут быть возложены еще и функции непрерывной интеграции и настройки такого ПО для обеспечения бесперебойности бизнес-процесса кибербезопасности, связанного с ним (это еще называют DevOps Development & Operations);

- *специалист по настройке правил в системах SIEM, SOAR, IRP* получает от заказчика вводные данные о работе информационных систем и затем составляет правила выявления инцидентов и реагирования на них в используемых в SOC-Центре системах. Это могут быть правила корреляции в системах SIEM, которые отвечают за обработку входящих сообщений от систем безопасности заказчика и за выстраивание этих разнородных событий в логически целостную «историю» для поиска возможной атаки. Также настраиваются правила автоматического реагирования, локализации, восстановления информационных систем при помощи SOAR и IRP решений. В случае, если для защиты заказчиков используются сигнатурные методы обнаружения угроз, например, антивирусы или системы обнаружения/предотвращения компьютерных вторжений, то данный специалист создает для них сигнатуры, т.е. описывает правила, по которым угроза должна быть обнаружена;

- *аналитик 1-го уровня* осуществляет первичную обработку киберинцидентов, или распределение и первичный отсев явных ложных срабатываний систем (такие события и инциденты называются ложноположительными). Специалисты 1-го уровня в работе опираются, как правило, на заранее созданные в SOC-Центре сценарии реагирования, в которых указана последовательность шагов, которые надо оперативно предпринять при поступлении того или иного типа инцидента. В случае, если аналитик 1-го уровня может самостоятельно выполнить все действия, он осуществляет

реагирование своими силами. Если он столкнулся с необходимостью эскалации инцидента, то он передает его на следующий уровень - аналитику 2-го уровня;

- *аналитик 2-го уровня* получает данные с 1-го уровня реагирования. Ему уже нужно не опираться на какие-то шаблоны реагирования, а анализировать уникальную ситуацию, применяя свою экспертизу и опыт расследования атак, сопоставляя различные события и факты, имеющие отношение к киберинциденту. В случае, если в расследуемой кибератаке применялось ранее неизвестное вредоносное ПО или вообще непонятно, что произошло, аналитик 2-го уровня эскалирует инцидент еще выше - специалисту по реверс-инжинирингу, форензик-эксперту или в специализированные компьютерные лаборатории;

- *специалист по реверс-инжинирингу* – эксперт высшей категории, как правило, профессиональный программист, решивший посвятить себя изучению образцов вредоносного программного кода для противодействия осуществляемым с их помощью кибератакам. Задача реверс-инженера состоит в том, чтобы понять, что делает и как устроен вирус: запустить вирус в изолированной среде (т.н. песочнице) для анализа его поведения, провести процедуру обратной разработки и получить из файла-образца первоначальный программный код, чтобы уже в нем найти особенности, которые помогут понять, что именно делает данный вирус и как ему лучше противостоять. При этом хакеры знают, что их вирус рано или поздно попадет к такому эксперту на исследование, и поэтому применяют техники запутывания (обфусцирования) кода, чтобы усложнить задачу реверс-инжиниринга;

- *форензик-эксперт* – это специалист по форензике (англ. forensics), т.е. компьютерной криминалистике. Эти специалисты могут понять, что изменилось в атакованной системе (компьютере, сервере, смартфоне), какие данные были стерты, изменены или похищены вирусом, какие еще системы в компании-заказчике были атакованы. Они даже способны воссоздать полный путь распространения угрозы, например, вируса: определить, на каком компьютере был этот вирус впервые запущен (чаще вирусы отправляют по email невнимательным сотрудникам), что именно он делал на зараженной системе (как правило, сначала вредонос «осматривается», пытаясь понять, куда попал, затем докачивает с сервера злоумышленников дополнительные компоненты, повышает свои права на атакованном ПК и начинает распространяться по сети компании), как затем развивалась атака и как был в итоге нанесен ущерб (чаще всего похищаются либо важная коммерческая информация, либо денежные средства со счетов организации);

- *специалист по кибервразведке* отвечает за поиск ранее не обнаруженных или затаившихся вредоносных программ в системах заказчиков (например,

вирусов-логических ловушек, которые срабатывают только при наступлении определенных условий, а до этого никак себя не проявляют). Также такой эксперт ищет в интернете, на специализированных закрытых форумах информацию о новых вирусах, новых киберпреступных группировках, пытается понять, не планируют ли злоумышленники массированную атаку на компанию-заказчика, нет ли «заказа» на кражу коммерческой информации защищаемой фирмы;

- *менеджер SOC* – это тот человек, который «переводит» техническую информацию об инциденте с языка ИТ и ИБ-специалистов на язык бизнеса, чтобы руководители компаний-заказчиков могли понять, насколько серьезным был ущерб или какую именно угрозу удалось предотвратить. SOC-менеджер также координируют работу всей команды SOC-Центра, связывает друг с другом заказчиков и исполнителей, выполняет организационную работу.

Для технического обеспечения информационной безопасности есть два принципиально разных подхода: ***превентивный и детективный***.

*Превентивный способ защиты информации* направлен на недопущение нарушения состояния информационной безопасности актива, например, блокирование запуска вредоносного файла антивирусом или запрет на входящее несанкционированное подключение межсетевым экраном. Таким образом, угрозы информационной безопасности пресекаются в истоке - всё направлено на сохранение информации с помощью превентивных (предотвращающих) средств.

Суть *детективного подхода* заключается в том, чтобы собрать как можно больше информации о некотором событии или действии, при условии, что мы точно не знаем, являются ли эти события или действия легитимными или нет.

Одним из ярких примеров таких обнаруживающих систем является система управления информацией о безопасности и событиями информационной безопасности – SIEM (Security Information and Event Management).

***SIEM - система*** накапливает в себе все данные (журналы работы «логи») от других средств защиты, умеющая понимать многие «форматы» логов из разных источников - средств защиты, быстро искать нужную информацию в этих логах, долгое время их хранить.

Кроме этого, SIEM-система должна уметь выполнять ряд дополнительных действий: осуществлять таксономию (распределять поступающие данные по типам и категориям) и корреляцию (т.е. связывать казалось бы разрозненные события между собой), отправлять уведомления ответственным лицам о выявленных подозрительных событиях в журналах, предоставлять дополнительную информацию по каждому из событий и устройств в сети.

Но как же выглядит работа системы SIEM на практике? Чтобы ответить на этот вопрос, сначала представим себе компанию среднего размера, с числом сотрудников около тысячи, каждый из которых работает за ПК, а важная информация и бизнес-системы хранятся и работают на серверах. В такой компании общее число типов технических систем защиты, как превентивных, так и детектирующих, легко может перевалить за десяток.

Рассмотрим распространенные типы средств защиты информации:

1. *Антивирусы* предотвращают выполнение вредоносного кода и деятельность вредоносного программного обеспечения на конечных точках (рабочих станциях и серверах), в локальном и веб-трафике, в электронной почте.

2. *Средства антиэксплойт защиты* позволяют обнаруживать и предотвращать вредоносное воздействие эксплойтов, т.е. программ или набора команд, использующих уязвимости установленного прикладного или системного программного обеспечения.

3. *Системы контроля и управления учетными записями* осуществляют централизованное управление учетными записями пользователей и администраторов ИТ-систем.

4. *Средства предотвращения утечек данных* предназначены для защиты от несанкционированной передачи ценной информации в нарушение установленных в компании правил - например, копирование рабочей информации на флешку или отправка на личную почту.

5. *Межсетевые экраны* (синоним брандмауэра или файерволла) контролируют входящий и исходящий сетевой трафик и в локальной сети, и в интернет. Цель контроля - разрешать нужный трафик легитимным приложениям и запрещать потенциально опасным.

6. *Системы обнаружения и/или предотвращения сетевых вторжений* предназначены для анализа сетевого трафика и поиска в нем признаков того, что устройство пытаются атаковать через сеть с применением эксплойтов. Как следует из названия, системы обнаружения вторжений только оповещают о возможной атаке, а системы предотвращения вторжений автоматически блокируют подозрительный трафик.

7. *«Песочницы»*, или средства изолированного выполнения программ позволяют запускать подозрительный файл в изолированной виртуальной среде, которая специально предназначена для поиска аномалий или потенциально вредоносного поведения исследуемого файла.

8. *Сканеры уязвимостей* предназначены для проведения анализа уязвимостей различных ИТ-систем путем получения данных об используемых версиях ПО и сравнением данной информации с каталогами известных уязвимостей, применимых к данным версиям.

9. *Системы ресурсов-приманок для злоумышленников* (honeypots и honeynets) представляют собой заранее созданные «муляжи» информационных систем, похожих на реальные системы компании, но не содержащих никаких ценных данных. Атакующие, попав в такую ловушку, попробуют применить свой инструментарий для проведения атаки, а в этот момент их действия будут тщательно журналироваться и затем изучаться специалистами по защите информации.

10. *Средства управления портативными устройствами* (MDM – Mobile Device Management) представляют собой программы для контроля и защиты портативных устройств сотрудников организации. Установив такое средство на свое устройство, сотрудник может получить контролируемый и безопасный удаленный доступ к ИТ-ресурсам организации, например, подключив себе на смартфон рабочую почту.

Типовая SIEM – система работает следующим образом:

Первая задача SIEM - получить данные от источника. Это может быть как «активный» источник, который сам умеет передавать данные в SIEM и ему достаточно указать сетевой адрес приемника, так и «пассивный», к которому SIEM-система должна обратиться сама. Получив от источника данные, SIEM-система преобразует их в единообразный, пригодный для дальнейшего использования формат – это называется нормализацией.

Далее SIEM-система выполняет таксономию, т.е. классифицирует уже нормализованные сообщения в зависимости от их содержания: какое событие говорит об успешной сетевой коммуникации, какое - о входе пользователя на ПК, а какое - о срабатывании антивируса. Таким образом, мы получаем уже не просто набор записей, а последовательность событий с определенным смыслом и временем наступления. Значит, что мы уже можем понять, в какой последовательности шли события и какая, может быть, связь между ними.

Тут в игру вступает основной механизм SIEM-систем: корреляция. Корреляция в SIEM — это соотнесение между собой событий, удовлетворяющих тем или иным условиям (правилам корреляции). Пример правила корреляции: если на двух и более ПК в течение 5 минут сработал антивирус, то это может свидетельствовать о вирусной атаке на компанию. Более сложное правило: если в течение 24 часов были зафиксированы чьи-то попытки удаленно зайти на сервер, которые в конце концов увенчались успехом, а затем с этого сервера началось копирование данных на внешний файлообменник, то это может свидетельствовать о том, что злоумышленники подобрали пароль к учетной записи, зашли внутрь сервера и крадут важные данные. По итогам срабатывания правил корреляции в SIEM-системе формируется инцидент информационной безопасности. При этом специалист по ИБ при работе с SIEM должен иметь

возможность быстрого поиска по хранящимся в SIEM-системе предыдущим инцидентам и событиям на случай, если ему потребуется узнать какие-либо дополнительные технические подробности для расследования атаки.

*Основные задачи SIEM-систем:*

1. Получение журналов с разнообразных средств защиты.
2. Нормализация полученных данных.
3. Таксономия нормализованных данных.
4. Корреляция классифицированных событий.
5. Создание инцидента, предоставление инструментов для проведения расследования.
6. Хранение информации о событиях и инцидентах в течение длительного времени (от 6 месяцев).
7. Быстрый поиск по хранящимся в SIEM данным.

Подводя итог, можно сказать, что системы SIEM необходимы организациям для работы с большим потоком разнородных данных от различных источников в целях выявления потенциальных инцидентов информационной безопасности и своевременного реагирования на них. Польза от внедрения и применения SIEM-системы заключается в том, что она значительно ускоряет процесс обработки инцидентов ИБ и получения требуемой информации о событиях ИБ: аналитику не нужно подключаться к каждому средству защиты информации, он видит все данные в едином, консолидированном виде в одном удобном интерфейсе.

## Раздел 3. УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

### 9. Система управления информационной безопасностью

В настоящее время принято рассматривать управление как процесс. Такое понимание распространяется и на область ИБ. Управление ИБ — это тоже процесс, представляющий собой логически взаимосвязанную между собой и непрерывную во времени последовательность работ, направленную на достижение поставленной специфичной цели организации информационной безопасности (ОИБ) [10-12].

***Управление ИБ*** организации представляет собой циклический процесс, состоящий из совокупно-целенаправленных действий, осуществляемых для достижения заявленных бизнес-целей организации посредством обеспечения защищенности ее информационной сферы, и включающий осознание необходимости организации информационной безопасности ОИБ, постановку задачи по ОИБ, оценку текущей ситуации и состояния объекта управления,

планирование мер по обработке рисков ИБ, реализацию, внедрение и оценку эффективности соответствующих защитных мероприятий и средств управления, распределение ролей и ответственности в области ОИБ, обучение и мотивацию сотрудников, выбор управляющих и корректирующих воздействий и их реализацию.

Управление ИБ организации — это не разовое мероприятие. Его следует рассматривать как непрерывную деятельность по постоянному поддержанию требуемого организацией уровня ИБ, так как правильно управляемая ИБ - инструмент успешного ведения деятельности предприятия.

Основными предметами управления ИБ в организации являются следующие области деятельности:

- планирование работ по ОИБ, включая разработку и продвижение соответствующей документации;
- поддержка и участие в эксплуатации защитных мер;
- осуществление контроля за ОИБ и уровнем ИБ;
- совершенствование работ по ОИБ на основе собственного опыта и применения на практике.

В целом процесс управления ИБ организации, имеющий циклический характер, заключается в следующем:

- описание объектов управления и защищаемых активов организации и сбор данных об их состоянии;
- выявление и формализация возможных угроз ИБ и анализ рисков ИБ;
- оценка защищенности объектов управления (с выявлением уязвимостей) и ее сравнение с требованиями по ОИБ организации, сформулированными в политиках информационной безопасности (ПолИБ);
- формирование управляющих воздействий;
- оценка результирующей деятельности по управлению ИБ.

Таким образом, управление ИБ в организации включает в себя две важнейшие составляющие — собственно сам процесс управления ИБ и систему управления ИБ (СУИБ) организации, которая подробно рассмотрена далее.

*Цель управления ИБ в организации* заключается в обеспечении осуществления соответствующих мероприятий таким образом, что в текущий момент надлежащим образом:

- снижены риски ИБ;
- осуществляются инвестиции в ОИБ;
- руководство ознакомлено со всеми осуществляемыми мероприятиями;
- верно сформулированы критерии оценки эффективности ОИБ.

***Основные задачи управления применительно к ИБ*** можно сформулировать таким образом:

*Целеполагание* (определение требуемого состояния или поведения) - ОИБ и соответствующего уровня ИБ организации на основе риск- ориентированного подхода (подразумевает отсутствие недопустимого риска ИБ) и выполнения требований законодательных и нормативных документов по ОИБ.

*Стабилизация* (удержание в существующем состоянии в условиях возмущающих воздействий) — выбор и реализация таких управляющих воздействий по ОИБ (планирование, внедрение и обслуживание защитных мер), которые позволят сохранить требуемый организации уровень ИБ в течение длительного времени.

*Выполнение программы* (перевод в требуемое состояние в условиях, когда значения управляемых величин изменяются по известным законам) - соблюдение планов обработки инцидентов ИБ и рисков ИБ, проведения аудитов ИБ, корректирующих действий в отношении деятельности ОИБ в соответствии с результатами аудитов ИБ и анализа данной деятельности со стороны руководства организации, ОИБ и многого другого, что было запланировано и входит в разнообразную деятельность по ОИБ.

*Слежение* (удержание требуемого состояния или поведения в условиях, когда законы изменения управляемых величин неизвестны или изменяются) - оценка по установленным критериям уровня ИБ в условиях изменения угроз ИБ, появления новых атак и обнаружения новых уязвимостей (управление рисками нарушения ИБ, контроль за соблюдением ПолИБ, самооценка и внутренний аудит ИБ, анализ работы СОВ и других систем) и поддержание требуемого уровня ИБ за счет реализации постоянных корректирующих воздействий (например, за счет оперативного изменения настроек СЗИ).

*Оптимизация* (удержание или перевод в состояние с экстремальными значениями характеристик при заданных условиях и ограничениях) - достижение экономической целесообразности в выборе защитных мер и поддержания всех процессов ОИБ.

Процесс управления ИБ организации реализуется СУИБ, включающей в себя помимо самого управляемого (защищаемого) объекта средства управления его состоянием, механизм сравнения текущего состояния с требуемым и средства формирования управляющих воздействий для локализации и предотвращения ущерба вследствие реализации угроз ИБ. Критерием управления в данном случае целесообразно считать минимум ущерба для активов организации при минимальных затратах на обеспечение их ИБ, а целью управления - обеспечение требуемого состояния активов (управляемого объекта) в смысле защищенности.

***Систему управления информационной безопасностью (СУИБ)*** (information security management system) рассматривают как часть общей

системы управления организации, основанную на подходе оценки и анализа бизнес-рисков, предназначенную для разработки, внедрения, эксплуатации, постоянного контроля, анализа, поддержания и улучшения ИБ, и включающую организационную структуру, политику, планирование действий, обязанности, установившийся порядок, процедуры, процессы и ресурсы в области ИБ [10-12].

СУИБ в организации выполняет следующие важнейшие функции:

- реализует целенаправленный, систематический и комплексный подход к управлению ИБ защищаемых активов, что приводит к повышению текущего уровня их защищенности;
- объединяет все применяемые в организации защитные и организационные меры в единый, адекватный реальным угрозам ИБ и управляемый комплекс, позволяющий достигать целей ОИБ на уровне всей организации;
- позволяет четко установить, как взаимосвязаны процессы и подсистемы ОИБ, кто за них отвечает, какие финансовые и трудовые ресурсы необходимы для их эффективного функционирования;
- проводит процесс выполнения ПолИБ и позволяет находить и устранять слабые места в ОИБ;
- охватывает людей, процессы и ИТ-структуру организации.

Наглядное представление основных компонентов СУИБ приведено в [10-12] (рис. 9.1). Процессы ОИБ поддерживаются ПолИБ и концепцией ОИБ, в которых сформулированы цели и стратегия ОИБ, а также организация самих процессов ОИБ. Следовательно, *СУИБ является неотъемлемой частью системы обеспечения ИБ (СОИБ).*


Рис. 9.1. Основные компоненты СУИБ

Область действия СУИБ, ее администрирование и ресурсы зависят от размеров организации и ее защищаемых активов.

Чтобы быть действительно полезной для организации, СУИБ должна быть эффективной. Правильно разработанная, должным образом реализованная и применяемая СУИБ позволяет не только вернуть затраченные на нее средства, но и внесет положительный вклад в успех деятельности организации.

Как показывает накопленный в данной области мировой и отечественный опыт, эксплуатация СУИБ дает организации ряд бесспорных выгод от ее использования:

- обеспечение соответствия уровня ИБ законодательным, отраслевым, контрактным, внутрикорпоративным требованиям и целям бизнеса;
- доказательство стремления высшего руководства к ОИБ в необходимом объеме для всей организации в соответствии с установленными требованиями;
- повышение доверия партнеров, клиентов, заказчиков за счет демонстрации высокого уровня ОИБ всем заинтересованным сторонам;
- управляемое ОИБ и контролируемое управление ИБ (особенно в критичных ситуациях);
- систематизация процессов ОИБ;
- расстановка приоритетов в области ИБ;
- достижение «прозрачности» ОИБ;
- обеспечение понятности защищаемых активов для руководства; выявление угроз ИБ для бизнес-процессов;
- достижение адекватности ОИБ существующим рискам;
- предупреждение возникновения инцидентов ИБ и снижение ущерба в случае их возникновения;
- повышение культуры ИБ в организации;
- интеграция защитных мер в бизнес-процессы;
- оптимизация (за счет формализации всех процессов ОИБ) и обоснование расходов на ИБ;
- снижение финансовых рисков и рисков прямых потерь;
- снижение операционных рисков за счет повышения экономической эффективности ОИБ;
- снижение рисков для инвесторов за счет повышения прозрачности процессов внутри организации;
- экономия времени, ресурсов и затрат на начальной стадии сбора информации при проведении любых аудитов ИБ;
- создание информации, порождаемой в процессе использования СУИБ, полезной для всех заинтересованных сторон и т. д.

Поскольку внедрение СУИБ требует значительных ресурсов, организации должны четко осознавать преимущества ее использования. Различные организации имеют разные бизнес-стимулы для этого, включая нормативную и правовую базу, статус (крупный или малый бизнес, общественная или государственная организация), географическое расположение, сферу деятельности (вид бизнеса) и предоставляемые ею услуги (или производимую продукцию) и т. п. Ранее уже подчеркивалось, что внедрение СУИБ должно стать стратегическим решением руководства организации. На ее проектирование и использование оказывают влияние потребности и цели, требования по ОИБ, применяемые процессы, а также размер и структура организации. Все эти элементы и поддерживающие их системы изменяются во времени. Поэтому и СУИБ будет также меняться соответственно потребностям организации. Деловая аргументация для внедрения СУИБ должна быть четко документирована и должна подробно излагать ожидаемые затраты в сравнении с выгодами, которые могут быть получены от увеличения возможностей управления ИБ. СУИБ не должна создаваться в изоляции, она должна учитывать все бизнес-риски и общие бизнес-стратегии организации [10-12].

## 10. Политики информационной безопасности

***Политика информационной безопасности ИБ (ПолИБ) организации*** - совокупность требований и правил по ОИБ для объекта ИБ, выработанных в соответствии с требованиями руководящих и нормативных документов в целях противодействия заданному множеству угроз ИБ, с учетом ценности защищаемой информационной сферы и стоимости СОИБ. Также в нее входят документированные решения в области ОИБ, совокупность (одно или несколько) документированных правил, процедур, практических приемов в области безопасности, которыми руководствуются организация в своей деятельности.

Политики ИБ делятся на ***корпоративные*** (верхнего уровня) и ***частные***.

*В широком смысле* корпоративная ПолИБ определяется как система документированных управленческих решений по ОИБ организации.

*В узком смысле* корпоративная ПолИБ – отдельный нормативный документ, определяющий требования безопасности, систему мер и порядок действий, а также ответственность сотрудников организации и средства управления для определения области ОИБ.

*Частная* ПолИБ, или ПолИБ по конкретным вопросам или проблемам, или ПолИБ по конкретным системам, ориентированная на отдельную область ОИБ или технологию, используемую в организации или ее подразделении.

Содержание политики ИБ в общем виде приведено на рисунке 10.1.

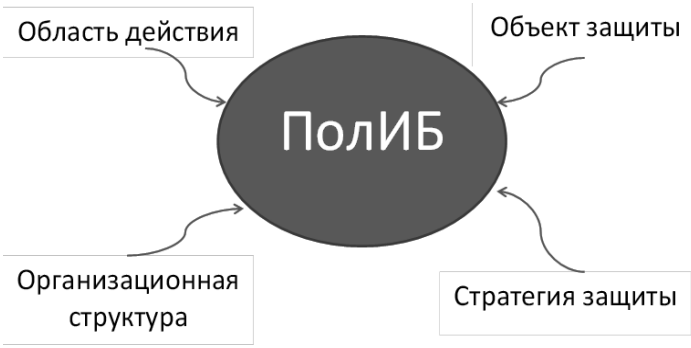


Рис. 10.1. Содержание ПолИБ организации

Корпоративная ПолИБ как политика верхнего уровня должна включать в себя следующие разделы:

***Цель (назначение).*** Корпоративная ПолИБ обычно содержит утверждение, поясняющее, зачем она была разработана. Всегда полезно явно указать цель или причины ее написания. Например, если организация предоставляет услуги по поддержке больших баз данных (БД), тогда ее основными целями могут быть снижение числа ошибок, потери и искажения данных, а также быстрота восстановления после нештатных ситуаций. Для организации, обрабатывающей персональные данные, первостепенной задачей может быть усиленная защита от несанкционированного раскрытия информации о клиентах. Поэтому типовыми являются *следующие цели:*

- обеспечение устойчивого функционирования организации за счет предотвращения реализации угроз ИБ ее активам, защита законных интересов владельца информации от противоправных посягательств, обеспечении нормальной производственной деятельности всех подразделений организации;
- обеспечение уровня ИБ в конкретных функциональных областях, соответствующего нормативным документам организации и рассчитанного на основе риск-ориентированного подхода (с учетом результатов оценки рисков ИБ);
- выработка планов восстановления после критических ситуаций и ОНБ организации и другие;
- достижение экономической целесообразности в выборе защитных мер;

- реализация подотчетности анализа регистрационной информации и всех действий пользователей с информационными ресурсами.

Задачами ОИБ являются все действия, которые необходимо выполнить для достижения поставленных целей. В частности, необходимо решать такие задачи, как анализ и управление рисками ИБ, расследование инцидентов ИБ, разработка и внедрение планов ОНБ, повышение квалификации и осведомленности сотрудников в области ИБ.

***Область действия***. Перед изложением самой ПолИБ определяется область ее действия с помощью ограничений и условий в понятных всем терминах, которые вводятся в явном виде. Надо уточнить, где, как, когда, кем и к чему применяется данная ПолИБ. Если, например, говорить о ПолИБ при подключении организации к Интернету, то может понадобиться уточнение, какие соединения, через которые ведется работа с Интернетом (напрямую или опосредованно), охватывает эта политика. ПолИБ также может определять, учитываются ли другие аспекты работы в Интернете, такие как соединение с Интернетом с домашнего компьютера.

ПолИБ точно определяет, какие активы организации она затрагивает, в том числе персонал, информацию, программное обеспечение (ПО) и аппаратное обеспечение (АО), устройства, технологии и т. п. Например, защищаемые в рамках ПолИБ активы организации можно описать так: «Положения настоящей ПолИБ распространяются на все виды информации, хранящиеся или передающиеся в организации, в том числе на информацию, зафиксированную на материальных носителях или передающуюся в устной или визуальной форме». Но во многих случаях корпоративная ПолИБ имеет отношение ко всем системам и всем сотрудникам организации без исключения.

***Основные положения ПолИБ.*** В явной форме описывается позиция организации (то есть решение ее руководства) по данному вопросу. Позиция может быть сформулирована как в наиболее общем виде как набор целей, которые преследует организация в данном аспекте, так и конкретизирована.

В ПолИБ требуется кратко описать все процессы и процедуры системы управления (СУИБ). В частности, выделяются такие процедуры, как контроль доступа к активам организации, внесение изменений в ее ИС, взаимодействие с третьими лицами, повышение квалификации сотрудников в области ИБ, расследование инцидентов ИБ, аудит ИБ. В описании каждой процедуры необходимо четко определить цели и задачи процедуры, основные правила ее выполнения, регулярность или сроки выполнения.

Перечисляются конкретные меры, реализующие ПолИБ в организации, дается обоснование выбора именно такого перечня мер и указывается, какие

угрозы ИБ для активов наиболее эффективно предотвращаются данными защитными мерами.

С целью формализации процесса управления ИБ в соответствии с ПолИБ требуется создание организационной структуры, которую также требуется описать.

Необходимо предусмотреть период пересмотра ПолИБ, что может быть изложено, например, следующим образом: «Положения Политики ИБ требуют регулярного пересмотра и корректировки не реже одного раза в полгода.

Внеплановый пересмотр Политики ИБ проводится в случаях:

- существенных изменений в национальной законодательной базе в области ИБ;
- внесения существенных изменений в интранет (изолированную от Интернета часть) организации;
- возникновения инцидентов ИБ.

При внесении изменений в положения Политики ИБ организации учитываются:

- результаты анализа функционирования СУИБ со стороны руководства организации;
- результаты аудита ИБ (внешнего и внутреннего);
- рекомендации независимых экспертов по ИБ.

***Ответственность (роли и обязанности).*** В этом разделе ПолИБ точно устанавливается, кто и за что отвечает. Указывается, на кого конкретно возлагается ответственность за соблюдение ПолИБ (например, менеджеров, владельцев активов, пользователей, администраторов систем и т. д.). Если для использования ПО сотрудникам требуется разрешение руководства, должно быть известно, у кого и как его можно получить.

Для ПолИБ уместно описание (с краткой детализацией) нарушений, которые неприемлемы, и последствий такого поведения. Могут быть явно перечислены наказания, применяемые к нарушителям ПолИБ (предварительно их нужно согласовывать с соответствующими должностными лицами и отделами, законодательными актами).

За нарушение ПолИБ должны быть предусмотрены конкретные дисциплинарные, административные взыскания и материальная ответственность. Но при этом нельзя забывать, что нарушения ПолИБ бывают и непреднамеренными со стороны сотрудников - они могут быть связаны, например, с отсутствием соответствующих знаний.

Устанавливаются как организационные, так и технические меры реагирования на нарушение ПолИБ. Эти меры предусматривают оповещение об инциденте ИБ, соответствующую реакцию, процедуры восстановления, сбор

доказательств, проведение расследования и привлечение нарушителя к ответственности. Система мер по реагированию на инциденты ИБ должна быть скоординирована между ИТ-департаментом, службой безопасности и службой персонала.

Также стоит поставить задачу конкретному подразделению организации следить за соблюдением ПолИБ. Кроме этого, приводится информация о должностных лицах, ответственных за реализацию ПолИБ, и четко устанавливаются их обязанности в отношении разработки и внедрения различных аспектов ПолИБ, а также в случае нарушения политики. Обязанность за общее управление ИБ возлагается на руководство организации. Ответственность сторонних пользователей обязательно оговаривается в соответствующих договорах. Отдельно описывается ответственность за контроль соблюдения ПолИБ.

***Соблюдение ПолИБ***. Это выражается в соблюдении двух видов соответствий:

1. Общее соответствие, обеспечивающее выполнение требований по разработке ПолИБ и определению ответственности, возложенной на различные организационные структуры поддержания ИБ.

2. Использование только установленных наказаний и дисциплинарных мер. Поскольку ПолИБ — это высокоуровневый документ, то конкретные меры наказания за различные нарушения, как правило, не детализированы в корпоративной ПолИБ.

***Ответственные (консультанты) по вопросам ИБ и справочная информация.*** Для любой ПолИБ нужны консультанты, с кем можно связаться в случае необходимости и получить квалифицированную помощь, разъяснения и дополнительную информацию по вопросам ОИБ. В зависимости от задачи, консультантом может выступать сотрудник соответствующего отдела. Например, по некоторым вопросам консультантом может быть один из менеджеров, по другим - начальник отдела, сотрудник технического отдела, системный администратор или сотрудник службы ИБ. Они должны уметь разъяснять положения ПолИБ и правила работы с конкретной системой. В их обязанности входит ознакомление всех новых сотрудников организации с ПолИБ при устройстве на работу и уведомление об изменениях в политике по мере их внесения. Также должно вестись обучение всех сотрудников основным вопросам ОИБ, а администратор и сотрудники отдела ИБ организации должны регулярно проходить переподготовку с целью повышения квалификации в специализирующихся в этих вопросах учебных заведениях.

Содержания частных ПолИБ по перечню разделов не отличаются от таковых для корпоративной ПолИБ. Все их положения ни в коем случае не

должны вступать в противоречия с корпоративной ПолИБ и формируются на основании принципов, требований и задач, определенных в корпоративной ПолИБ, с учетом:

- детализации, уточнения и дополнительной классификации активов и угроз ИБ;
- определения владельцев защищаемых активов;
- оценки рисков ИБ и возможных последствий реализаций угроз ИБ в границах области действия регламентируемой политикой области, системы, технологии, подразделения и т. п.

Не рекомендуется повторение одинаковых правил в различных частных политиках. Включение в частную ПолИБ правила, содержащегося в другой существующей политике, целесообразно осуществлять посредством соответствующей ссылки.

Частные ПолИБ определяют следующее:

- цели и задачи ОИБ, на обеспечение которых направлена частная ПолИБ;
- область действия, определение объектов защиты, уязвимостей, угроз ИБ и оценка рисков ИБ, связанных с объектами защиты;
- сведения о виде деятельности, на ОИБ которой направленно действие положений частной ПолИБ, совокупности банковских технологий, применяемых в рамках выполнение данного вида деятельности, и основных технологических процессов, реализующих указанные технологии;
- определение субъектов (ролей), на которых распространяется действие политики (как структурных подразделений организации, так и отдельных исполнителей);
- содержательную часть (требования и правила);
- обязанности по ОИБ в рамках области действия частной ПолИБ, описание функций субъектов (ролей) над управляемыми объектами в рамках регламентируемых технологических процессов;
- состав ссылочных документов (документы, ознакомление с которыми обязательно для полноценного понимания текста политики);
- положения по контролю реализации политики;
- ответственность за реализацию и поддержку политики;
- условия пересмотра политики.

Чаще всего в организации разрабатывается одна корпоративная политика ИБ и несколько частных политик (по конкретным вопросам и системам).

## 11.Анализ и управление рисками информационной безопасности

***Риск информационной безопасности*** – это потенциальная возможность использования уязвимостей активов конкретной угрозой для причинения ущерба организации.

Величина риска:

$$R_E = P_E \cdot M_D, \qquad 11.1$$

где $P_E$ – вероятность события,
$M_D$ – размер ущерба.

Вероятность события вычисляется по формуле:

$$P_E = P_T \cdot M_V, \qquad 11.2$$

где $P_T$ – вероятность угрозы,
$M_V$ – величина уязвимости.

Цели процесса анализа рисков ИБ:

1. Идентифицировать активы и оценить их ценность.
2. Идентифицировать угрозы активам и уязвимости в системе защиты.
3. Просчитать вероятность реализации угроз и их влияние на деятельность организации.
4. Соблюсти баланс между стоимостью возможных негативных последствий и стоимостью мер защиты, дать рекомендации руководству компании по обработке выявленных рисков.

Этапы 1–3 - ***оценка риска,*** этап 4 - ***анализ рисков.***

Способы обработки риска ИБ:

- игнорировать;
- принять;
- избежать;
- передать;
-минимизировать.

Существуют *количественный* и *качественный* способы анализа рисков ИБ.

***Количественные способы*** используются с целью расчетов конкретных величин, выраженных в числовых значениях, процентах. Опираются на сравнение с эталонными величинами, которые заранее известны и приемлемы. При количественном подходе каждому виду риска присваивается конкретная величина и параметры, выраженные в денежных, временных эквивалентах. Это облегчает понимание ситуации, позволяет оценить возможный ущерб, расходы

на обеспечение защитных мер, долю резервов, которые придется задействовать. Для начала необходимо провести оценку всех информационных активов компании в денежном эквиваленте для понимания их важности и критичности. После этого проводится определение величин возможного ущерба в случае конкретных рисков и отдельных информационных активов. Следующим шагом станет расчет вероятности наступления каждой возможной угрозы в отношении активов. Далее рассчитывают суммарный потенциальный ущерб для каждого вида угроз с привязкой к какому-то временному периоду. В конце выполняют анализ собранных данных и определяют количественный размер ущерба применительно к конкретной угрозе.

***Качественные*** основываются на присвоении риску определенного ранга согласно системе ценностей: баллы, степени. Сначала выставляется оценка ценности информационных активов. Потом рассчитывается вероятность наступления угрозы по отношению к активу. Далее рассчитывают вероятность реализации угрозы, принимая во внимание действующие защитные меры. После этого делается вывод о размере риска, исходя из ценности конкретного актива, а также вероятности наступления риска. В конце проводится анализ и выставляется оценка в отношении каждой угрозы, величины риска. Также разрабатываются защитные меры по каждой угрозе для снижения величины ущерба.

***Процедуры управления риском:***

1. *Идентификация риска:*
   - анализ базы событий;
   - самооценка;
   - анализ динамики количественных показателей (ключевых индикаторов риска);
   - анализ результатов регуляторных проверок;
   - анализ результатов внешнего аудита;
   - анализ поступающих сигналов от сотрудников.
2. *Сбор и регистрация информации о событиях риска:*
   - автоматизированное (из информационных систем), неавтоматизированное (экспертным методом), алгоритмизированное выявление информации о рисках;
   - классификация рисковых событий;
   - оценка потерь, стоимости возмещения потерь;
   - регистрация рисковых событий в базе событий;
   - обновление информации, актуализация источников информации.
3. *Количественная и качественная оценка уровней риска:*
   - организации сами разрабатывают способы оценки.

*4. Выбор и применение способов реагирования на риск.*
*5. Мониторинг рисков:*
- анализ индикаторов риска и статистики;
- контроль выполнения мероприятий;
- мониторинг входящей информации.

В организации рекомендуется сначала внедрить политику управления рисками ИБ и методологию оценки рисков ИБ и провести первоначальную высокоуровневую оценку рисков вручную, а затем перейти к выбору инструментов, которые бы соответствовали выбранному подходу и облегчали выполнение основных операций по оценке рисков ИБ. Положительный эффект от использования таких инструментов может быть значительно выше при детальной оценке рисков ИБ, предполагающей рассмотрение большого количества рисков, так как в этом случае аналитическая работа существенно усложняется.

## 12. Кадровые и организационные вопросы информационной безопасности

***Главная цель организационного управления ИБ*** – наиболее продуктивным способом объединить существующие в организации структуры и культуру с новой деятельностью по разработке и внедрению системы обеспечения ИБ. Это достигается за счет определения и классифицирования существующей в организации структуры как соответствующей определенному типу управления ИБ.

Организационное управление ИБ определяет способ, которым ИБ передается под контроль, реализуется и управляется во всей организации. Управление может быть, как правило, централизованным или децентрализованным, но эти категории специально упрощаются для практических целей построения модели организационного управления ИБ. Причина состоит в том, что многие объекты должны применять сразу оба атрибута для достижения организации ИБ экономически эффективным образом, и, таким образом, они часто в одно и то же время централизованы и децентрализованы. Это можно смоделировать, признав, что управление ИБ заключается в двух основных видах деятельности – руководстве и администрировании, каждый из которых может быть как централизованным и децентрализованным.

Руководство относится к органу управления ИБ, имеющему соответствующие компетенции и полномочия для принятия решений по управлению ИБ в интересах организации.

Администрирование относится к органу управления, применяющему, собственно управляющему и обеспечивающему исполнение деятельности по организации ИБ в соответствии с тем, как это предписано.

Централизация указывает на наличие единого органа, который может быть отдельным лицом, комитетом или другой структурной единицей.

Децентрализация подразумевает наличие нескольких органов с одинаковым уровнем полномочий.

На этой основе можно разработать четыре базовых модели организационного управления ИБ:

1) Централизованное руководство / централизованное администрирование;

2) Централизованное руководство / децентрализованное администрирование;

3) Децентрализованное руководство / централизованное администрирование;

4) Децентрализованное руководство / децентрализованное администрирование.

Пример рассмотрения базовой модели «Централизованное руководство/централизованное администрирование» представлен на рис. 12.1.

Централизованное руководство (ЦР) указывает на такую организацию руководства, где полномочия по принятию решений в области политики и бюджета, распространяемые на всю организацию, предоставляются одному представителю или собранию.

Централизованное администрирование (ЦА) предоставляют органу управления право применять и управлять ПолИБ управленческому персоналу ИБ или систем, которые последовательно (по единой цепочке) подчинены друг другу.

Централизованное руководство/централизованное администрирование (ЦР/ЦА) - один центральный орган управления ИБ отвечает за разработку политик, применяемых во всей организации; все административные функции управления ИБ выполняются персоналом в рамках одной цепочки подчиненности.

Этот тип управления соответствует полной централизации всей деятельности в области ИБ. Одно лицо из высшего руководства отвечает за разработку политик, применяемых во всей организации. Персонал в рамках одной цепочки подчиненности выполняет все административные функции по управлению ИБ. Все подразделения организации делегируют своих представителей в комитет по управлению вопросами ИБ, что обеспечивает их

достаточное влияние на принятие политических решений в области ИБ (это влияние изображено большими стрелками).

В этом случае Исполнительный директор определяет, что Управляющий директор отвечает за исполнение утвержденной программы обеспечения ИБ. Управляющий директор назначает ответственного на должность Директора службы ИБ. Комитет по управлению вопросами ИБ существует для гарантии того, чтобы каждое подразделение организации могло должным образом влиять на процесс принятия решений, поскольку в каждом подразделении возникают вопросы, связанные с ИБ, которые необходимо учитывать.

Сопровождение ИБ и ИТ полностью разделено и осуществляется параллельно: директор службы ИБ отвечает за все вопросы ИБ, а директор службы информатизации – за использование и обслуживание ИТ. Их обязанности не пересекаются, хотя зона ответственности распространяется на одно и то же аппаратное и программное обеспечение.

Количественный состав службы ИБ различен и зависит, прежде всего, от возможностей самой организации.

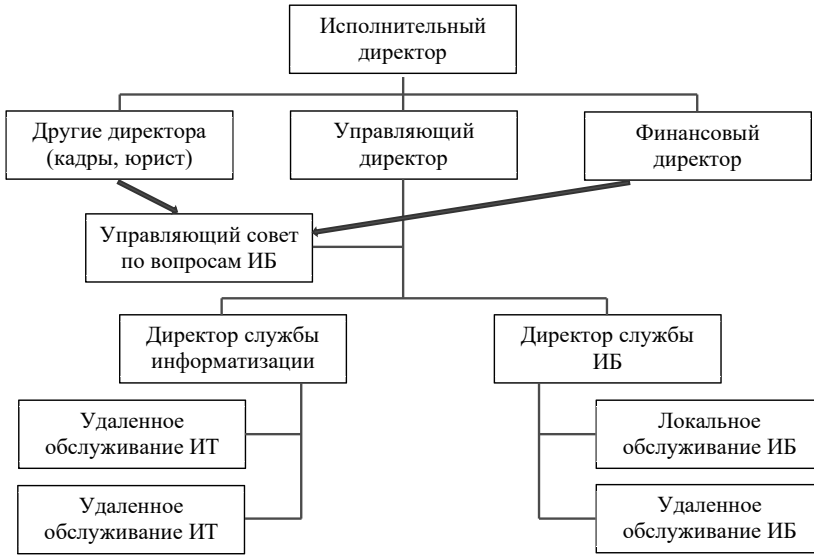


Рис. 12.1. Модель централизированного руководства / централизированного администрирования ИБ

В состав службы ИБ должны входить специалисты, которые определяют конкретные функциональные обязанности или роли по управлению ИБ в организации:

*Руководитель/начальник или директор (заместитель директора) службы ИБ),* непосредственно подчиненный главе организации и отвечающий за состояние всех видов безопасности, включая ИБ, организацию работ по созданию СОИБ и управлению ИБ в организации и руководящий соответствующим персоналом. В его обязанности входит разработка и поддержка эффективных защитных мер при обработке информации для обеспечения сохранности данных, АО и ПО, контроль за выполнением плана восстановления, общее руководство административными группами в подсистемах ИС при децентрализованном управлении.

*Заместитель начальника службы ИБ* - па некоторых предприятиях он руководит всеми видами безопасности или только физической, а иногда и технической службами охраны.

*Архитектор ИБ,* направляющий всю работу по ИБ в организации и предлагающий соответствующие инфраструктурные и архитектурные решения.

*Аналитики по вопросам ИБ,* отвечающие за анализ состояния ИБ, определение требований по ОИБ к различным подсистемам АС и путей обеспечения их защиты, а также за разработку необходимых нормативно-методических и организационно-распорядительных документов по вопросам ИБ.

*Риск-менеджер,* проводящий оценку рисков ИБ в организации, выбирающий для этого адекватные методы и предлагающий способы обработки имеющихся рисков.

*Криптоаналитик,* анализирующий зашифрованную информацию.

*Криптограф,* защищающий информацию организации посредством применения криптографических методов.

*Ответственные за работу с персональными данными*.

*Сотрудники физической охраны и пропускного режима* (по найму), но подчиненные руководителю службы безопасности.

*Администраторы средств защиты, контроля и управления,* отвечающие за сопровождение и администрирование конкретных средств защиты информации (СЗИ) и средств анализа защищенности.

*Сотрудник службы ИБ. ответственный за решение вопросов ИБ в разрабатываемых и внедряемых АО и ПО,* участвующий в разработке и реализации ПолИБ и защитных мер, технических заданий по вопросам ИБ, выборе средств и методов защиты, испытаниях новых средств с целью проверки выполнения требований по ОИБ, контролирующий защиту наборов данных и

ПО, оказывающий помощь пользователям и организующий общую поддержку групп управления ИБ в своей зоне ответственности и т. д. При децентрализованном управлении каждая подсистема ИС имеет своего сотрудника службы ИБ.

*Администратор ИБ,* участвующий в разработке и внедряющий СЗИ, которые обнаруживают, предотвращают, изолируют или снижают риски ИБ; поддерживающий в актуальном состоянии средства и меры защиты, а также устанавливающий и обеспечивающий правила разграничения доступа. Иногда также различают *администраторов ИБ систем,* контролирующих работу своей системы, следящих за выполнением планов непрерывной работы и восстановления, за хранением резервных копий, и *администраторов ИБ данных,* осуществляющих контроль за состоянием защиты наборов данных, ужесточающих защиту в случае необходимости, а также координирующих работу с другими администраторами.

*Член группы расследования инцидентов ИБ (ГРИИБ),* работающий в ГРИИБ для подготовки и обеспечения быстрого реагирования в случае возникновения инцидентов ИБ.

*Специалист по восстановлению,* разрабатывающий и внедряющий планы ОИБ и восстановления данных после инцидентов ИБ и чрезвычайных ситуаций.

*Юрист и технический специалист по компьютерным преступлениям/сотрудник отдела компьютерной форензики*, которые идентифицируют, выделяют, сохраняют и документируют свидетельства инцидентов ИБ.

*Тестировщик ИБ,* который планирует и, по согласованию с руководством, проводит проверочные тесты па проникновения в системы.

*Внутренний аудитор ИБ,* оценивающий адекватность и эффективность ОИБ организации, соответствие стандартам, политикам и т. д.

*Техник по компьютерным вирусам* анализирует информацию по только что обнаруженным вирусам и предлагает способы борьбы с ними до выхода официальных обновлений производителей антивирусов.

Перечень необходимых знаний и навыков, а также функциональных обязанностей лиц, входящих в службу и отдельную группу защиты информации, может существенно отличаться в зависимости от назначения структуры и задач, решаемых в конкретной системе.

Рассмотрим два основных варианта создания службы ИБ в организации [10-12].

1. *Системные администраторы и администраторы прикладных систем, фактически выполняющие функции службы ИБ.* Это наиболее распространенная организационная структура органов ИБ для организаций, в которых отсутствуют

работники, занимающиеся только вопросами ИБ. Такие администраторы находятся в подчинении одной или нескольких ИТ-структур организации. У них много своих основных обязанностей, связанных с обеспечением работоспособности интранета. Тогда большинство из выше указанных функций службы ИБ не выполняется. Как правило, лицо, ответственное за контроль реализации этих функций, не назначается.

2. *Выделенные в организации работники или отдельное подразделение, основной задачей которого является организация обеспечения ИБ.* Они могут находиться в разных зонах подчиненности: в службе безопасности, ИТ-службе, службе внутреннего контроля, а также могут представлять собой самостоятельное подразделение, подчиненное высшему руководству организации.

2а. *Подразделение находится в структуре службы безопасности.* Это наиболее распространенный вариант, который обладает следующим основными достоинствами:

- может быть обеспечена реализация всех четырех функций ОИБ;
- может быть оказано эффективное влияние на выполнение дополнительных связанных с ИБ задач, в первую очередь курируемых другими подразделениями;
- могут с различной степенью эффективности решаться задачи, не связанные с деятельностью ИТ-подразделений. Это прежде всего относится к задачам согласования документов (заявок на доступ, проектов развития), к некоторым задачам независимого (прежде всего от ИТ-подразделений) аудита и мониторинга ИБ, к задачам эксплуатации СЗИ (при условии четкого разделении полномочий ИТ-подразделения и ИБ-подразделений), а также к задачам методической функции, не связанным с реализуемыми ИТ-подразделениями функциями.

2б. *Подразделение ИБ находится в ИТ-подразделении организации.* Основное достоинство такого достаточно распространенного на практике решения объясняется тем, что значительная часть вопросов ИБ связана с вопросами безопасности ИТ, что позволяет достичь максимального взаимопонимания между ИТ- и ИБ-подразделениями.

2в. *Подразделение ИБ находится в контрольно-ревизионной службе организации.* Два основных достоинства такого подхода: можно эффективно организовать решение задач аудита и контроля и можно набрать в подразделение ИБ высококвалифицированных специалистов (как правило, за счет относительно высокого уровня оплаты труда). Основной из недостатков - реализация всех остальных функций (кроме аудита) крайне затруднена. Как правило, в службах

контроля работают специалисты по финансовому контролю, и вопросы ИБ весьма далеки от решаемых ими проблем.

2г. *Подразделение ИБ является самостоятельным и подчиненным непосредственно высшим руководителям организации.* Такое организационное решение обладает значительными преимуществами перед всеми ранее рассмотренными. Независимое подразделение ИБ может эффективно в короткие сроки решать основные задачи координации деятельности в области ИБ всех служб организации, реализуя при этом комплексный подход, устраняя выявленные недостатки и проблемы. Это следует из анализа приведенных функций и задач ОИБ с точки зрения определения подразделений, к которым такие задачи относятся. Больше половины задач ОИБ относятся ко всем подразделениям организации, поэтому их эффективное решение зависит от степени самостоятельности (независимости) подразделения ИБ в структуре организации.

## Литература

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. М.: Стандартинформ, 2008. 12 с.

2. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. М.: Стандартинформ, 2007. 11 с.

3. Бабаш А.В., Шанкин Г.П. Криптография. /Под редакцией В.П. Шерстюка, Э.А. Применко. – М.: СОЛОН-ПРЕСС, 2007.

4. Баричев С.Г, Гончаров В.В., Серов Р.Е. Основы современной криптографии: Учебный курс. – М.: Горячая линия-Телеком, 2002.

5. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. Учебное пособие для вузов/. – М.: Горячая линия – Телеком, 2006. – 544 с.

6. Болелов Э.А. Криптографические методы защиты информации: Пособие по выполнению практических занятий. – М.: МГТУ ГА, 2010.

7. Болелов Э.А. Криптографические методы защиты информации: Пособие по выполнению лабораторных работ. – М.: МГТУ ГА, 2010.

8. Болелов Э.А. Криптографические методы защиты информации. Часть 1. Симметричные криптосистемы. – М.:МГТУ ГА, 2011.

9. Галатенко В.А. Основы информационной безопасности. М.: ИНТУИТ.РУ «Интернет-Университет Информационных Технологий», 2003. – 280 с.

10. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Основы управления информационной безопасностью. Учебное пособие для вузов. - М.: Горячая линия - Телеком, 2014.

11. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Технические, организационные и кадровые аспекты управления информационной безопасностью. Учебное пособие для вузов. - М.: Горячая линия - Телеком, 2014.

12. Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности. Учебное пособие для вузов. - М.: Горячая линия - Телеком, 2014.

## Содержание