В. И. Аверченков, М. Ю. Рытов
А. В. Кувыклин, М. В. Рудановский

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНОВ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ

учебное пособие

ФЛИНТА

УДК 347.775(075.8)
А19

Р е ц е н з е н т ы:
кафедра программного обеспечения вычислительной техники
и систем информационной безопасности
Курганского государственного университета;
доктор технических наук профессор *Еременко В.Т.*

Аверченков В.И.

А19 Аудит информационной безопасности органов исполнительной власти : учеб. пособие [электронный ресурс] / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, М.В. Рудановский. – 3-е изд., стереотип. – М. : ФЛИНТА, 2011. – 100 с. – (Серия «Организация и технология защиты информации»).

ISBN 978-5-9765-1277-1

Рассматриваются общие вопросы теории информационной безопасности, понятие аудита информационной безопасности, нормативно-правовая база России в области информационной безопасности, предложена методика аудита информационной безопасности органов исполнительной власти и органов местного самоуправления субъектов Российской Федерации. Кроме того, рассмотрены вопросы лицензирования деятельности по защите информации и сертификации средств защиты информации.

Руководящие технические материалы предназначены для руководителей и сотрудников служб безопасности и служб защиты информации органов исполнительной власти и органов местного самоуправления для подготовки и проведения внутреннего и обоснования необходимости проведения внешнего аудита информационной безопасности, а также могут быть полезны преподавателям и студентам, обучающимся по специальностям, связанным с информационной безопасностью.

УДК 347.775(075.8)

ISBN 978-5-9765-1277-1

Оглавление

1. Основы информационной безопасности

Наша эпоха знаменуется бурным развитием информационных технологий во всех сферах человеческой деятельности. Информация в современном мире стала важным стратегическим ресурсом государства, имеющим высокую стоимость. Этот факт вызывает стремление отдельных государств, ряда организаций и отдельных граждан получить личные выгоды за счет овладения информацией ограниченного доступа. Кроме того, успешное развитие государства, как, впрочем, и отдельной личности зависит от степени защиты собственных информационных ресурсов.

Важность обеспечения безопасности государства в информационной сфере определяется принятой 9 сентября 2000 года “Доктриной информационной безопасности Российской Федерации”: ”Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать”.

Особо остро стоит вопрос обеспечения информационной безопасности в органах государственной власти и органах местного самоуправления субъектов Российской Федерации. Об этом свидетельствуют многочисленные попытки криминальных элементов получить контроль над информационными ресурсами государственной системы управления для извлечения материальной выгоды и нанесения финансового ущерба государству. Кроме того, в исполнительных органах государственной власти и органах местного самоуправления важно обеспечить конституционные права граждан России на получение достоверной информации, на ее использование в интересах осуществления законной деятельности, а также на защиту информации, обеспечивающую их личную безопасность.

Противоборство государств в области информационных технологий, стремление криминальных структур противоправно использовать государственные ресурсы, наличие множества преднамеренных и случайных угроз информационным ресурсам вызывают необходимость создания комплексных систем защиты

информации элементов системы государственного управления Российской Федерации.

1.1. Основные положения, понятия и определения теории информационной безопасности

Одной из приоритетных задач обеспечения суверенитета Российской Федерации является реализация и совершенствование системы обеспечения ее информационной безопасности. Сложность решения этой проблемы обусловлена необходимостью создания целостной системы комплексной защиты информации, базирующейся на стройной её организации и регулярном управлении. ***Комплексная система защиты информации*** – это организационно-техническая система, в которой действуют в единой совокупности правовые, организационные, технические, программно–аппаратные и другие нормы, методы, способы и средства, обеспечивающие защиту информации от всех потенциально возможных и выявленных угроз и каналов утечки.

В соответствии с законодательством Российской Федерации информацию по режиму доступа подразделяют на открытую, конфиденциальную информацию и государственную тайну.

Конфиденциальная информация - документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации. По содержанию конфиденциальная информация может иметь профессиональный, личный, служебный, банковский и другой характер.

Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны. Органы государственной власти, федеральные органы и органы местного самоуправления обеспечивают защиту

сведений, составляющих государственную и служебную тайну, в соответствии с возложенными на них задачами и в пределах своей компетенции, ответственность за организацию защиты сведений, составляющих государственную тайну, непосредственно возлагается на их руководителей.

Под ***защитой информации (ЗИ)*** понимают деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию [2].

Структурно-типовая система защиты информации (рис.1.1) представляет собой совокупность отдельных взаимосвязанных элементов, реализующих следующие её виды:

Правовая защита информации – защита информации, базирующаяся на применении статей конституции и законов государства, положений гражданского и уголовного кодексов и других нормативно-правовых документов в области информатики, информационных отношений и защиты информации. Правовая защита информации регламентирует права и обязанности субъектов информационных отношений, правовой статус органов, технических средств и способов защиты информации и является основой для морально – этических норм в области защиты информации [4].

Организационная защита информации – это комплекс направлений и методов управленческого, ограничительного и технологического характера, определяющих основы и содержание *системы защиты,* побуждающих персонал соблюдать правила защиты конфиденциальной информации. Организационные меры связаны с установлением *режима конфиденциальности* в организации [2].

Техническая или ***инженерно-техническая*** защита, основывается на использовании технических устройств, узлов, блоков, элементов, систем как в виде отдельных средств, так и встроенных в процессе единого технологического цикла создания средств обработки информации, сооружений и т.д.;

Программно-аппаратная защита предполагает использование программного обеспечения информационных систем, комплексов и систем, а также аппаратных устройств, встроенных в состав технических средств и систем обработки информации.

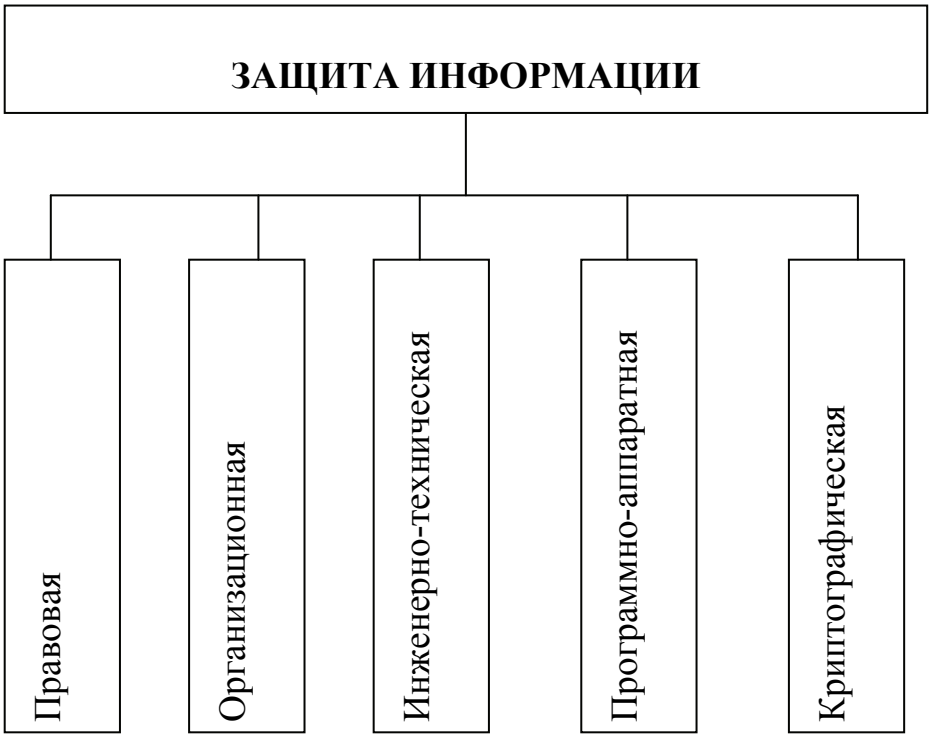

Рис.1.1. Структура типовой системы защиты

В качестве отдельного вида наиболее эффективных средств защиты информации выделяются ***математические*** или ***криптографические*** *методы,* которые могут быть реализованы в виде технических устройств, программ и программно-аппаратных средств.

Рассмотренные виды в основном обеспечивают надежную защиту информации в различных системах ее обработки и различных условиях их функционирования. Однако опыт практического обеспечения безопасности информации в России и за рубежом показывает, что для надежной защиты в условиях обязательного участия человека, массовости решения задач защиты необходимо, прежде всего, реализовывать организационно-правовые направления защиты информации.

Таким образом, при правильной организации комплексной системы защиты в организации создается система информационной безопасности.

Информационная безопасность **(ИБ)** – это состояние защищенности информационной среды организации, обеспечивающее его функционирование и развитие в соответствии с его целями и задачами. При построении системы информационной безопасности учитывают целый ряд компонентов, наиболее важными среди них являются следующие [3]:

- объекты угроз;
- угрозы;
- источники угроз;
- источники конфиденциальной информации;
- способы несанкционированного доступа к конфиденциальной информации;
- направления, методы и средства защиты информации.

В обобщенном виде рассмотренные компоненты в виде концептуальной модели безопасности информации приведены на следующей схеме (рис. 1.2.).

Объектом угроз информационной безопасности выступают сведения о составе, состоянии и деятельности объекта защиты (персонала, материальных и финансовых ценностей, информационных ресурсах).

Угрозы информации выражаются в нарушении ее целостности, конфиденциальности, полноты и доступности. Виды угроз информации приведены на рис.1.3.

Источниками угроз выступают международные террористические организации, организованные преступные группировки, спецслужбы иностранных государств, коррупционеры и различного рода злоумышленники.

Источники угроз преследуют при этом следующие цели - ознакомление с охраняемыми сведениями, их модификация в корыстных целях и уничтожение для нанесения прямого материального ущерба.

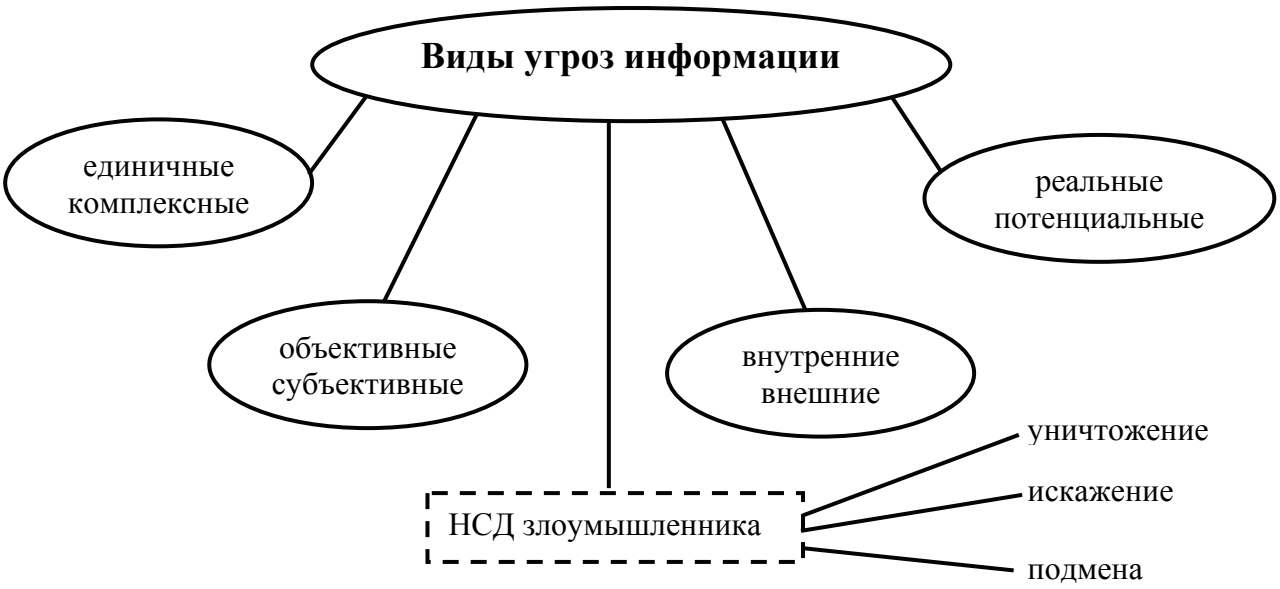

Рис. 1.3. Виды угроз информации (НСД – несанкционированный доступ)

В том случае, когда речь идет об утрате информации по вине персонала, используется термин «разглашение (огласка) информации». Человек может разглашать информацию устно, письменно, с помощью жестов, мимики, условных сигналов, лично, через посредников, по каналам связи и т.д. Термин «утечка информации», хотя и используется наиболее широко, однако в большей степени относится к утрате информации за счет ее перехвата с помощью технических средств разведки, по техническим каналам [6].

Неправомерное овладение конфиденциальной информацией возможно путем ее разглашения источниками сведений, утечки информации через технические средства и несанкционированного доступа к информационным ресурсам.

Обязательным условием успешного осуществления попытки несанкционированного доступа к информационным ресурсам ограниченного доступа является интерес к ним со стороны преступников и спецслужб. При отсутствии такого интереса угроза информации не возникает даже в том случае, если создались предпосылки для ознакомления с ней постороннего лица. Основным виновником несанкционированного доступа к информационным ресурсам является, как правило, персонал, работающий с документами и информационными ресурсами.

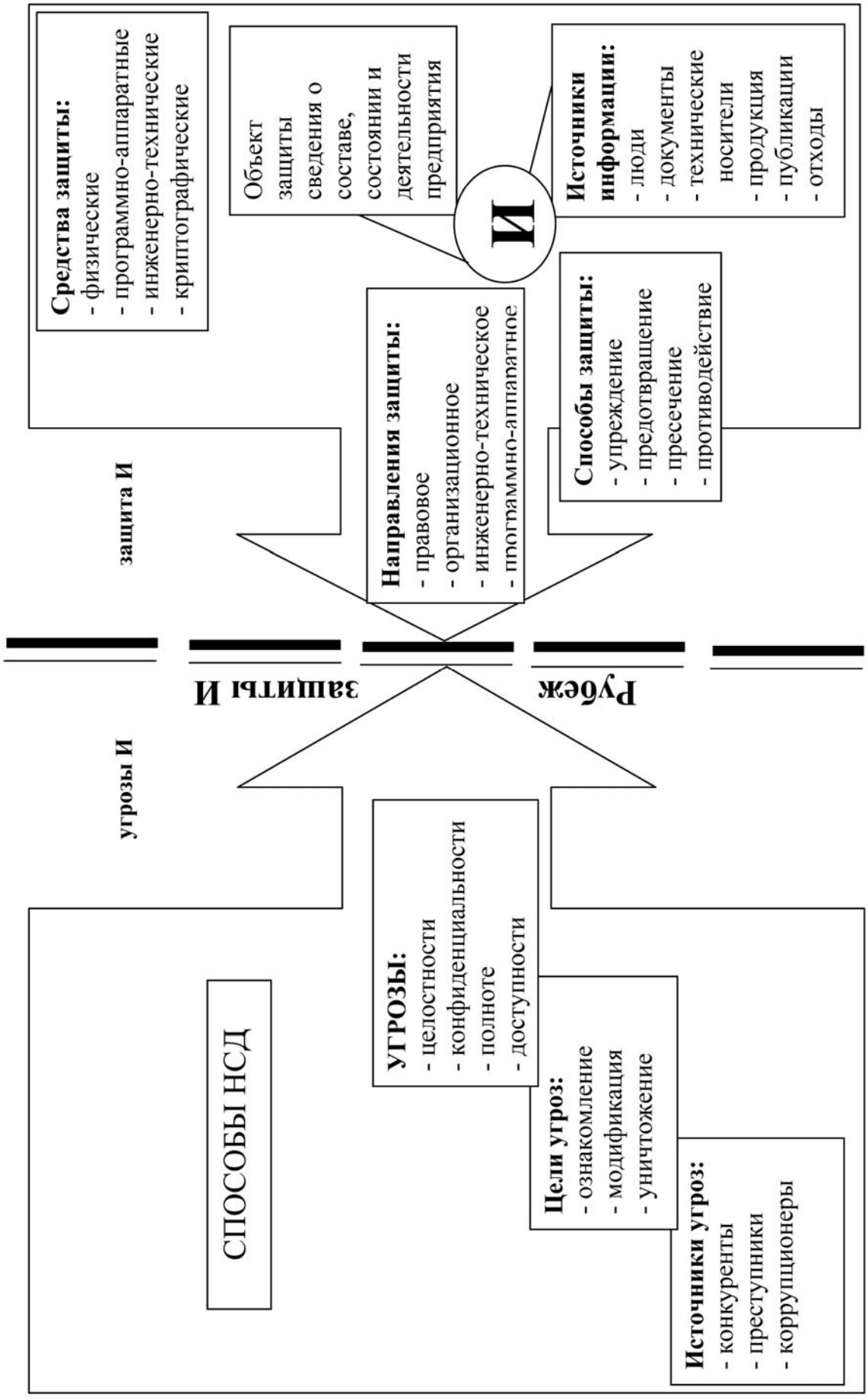

Рис. 1.2. Концептуальная модель информационной безопасности (И- информация)