СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

Р.Р. Фаткиева

Основы построения защищенных компьютерных сетей

Введение

СПбГЭТУ «ЛЭТИ», 2022 г.

1 ВВЕДЕНИЕ. ОСНОВНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ СИСТЕМ

Актуальность. От эффективности функционирования современных компьютерных сетей во многом зависит успешность деятельности практически во всех сферах общества (Рис. 1). С каждым годом происходит увеличение пространственно-временной конфигурации сценариев атак, особенностями которых являются наличие мощности атаки, позволяющей осуществить либо массированный удар на атакуемый ресурс (например, Ddos-атака), либо осуществить скрытое воздействие для проникновения в заданный объект.

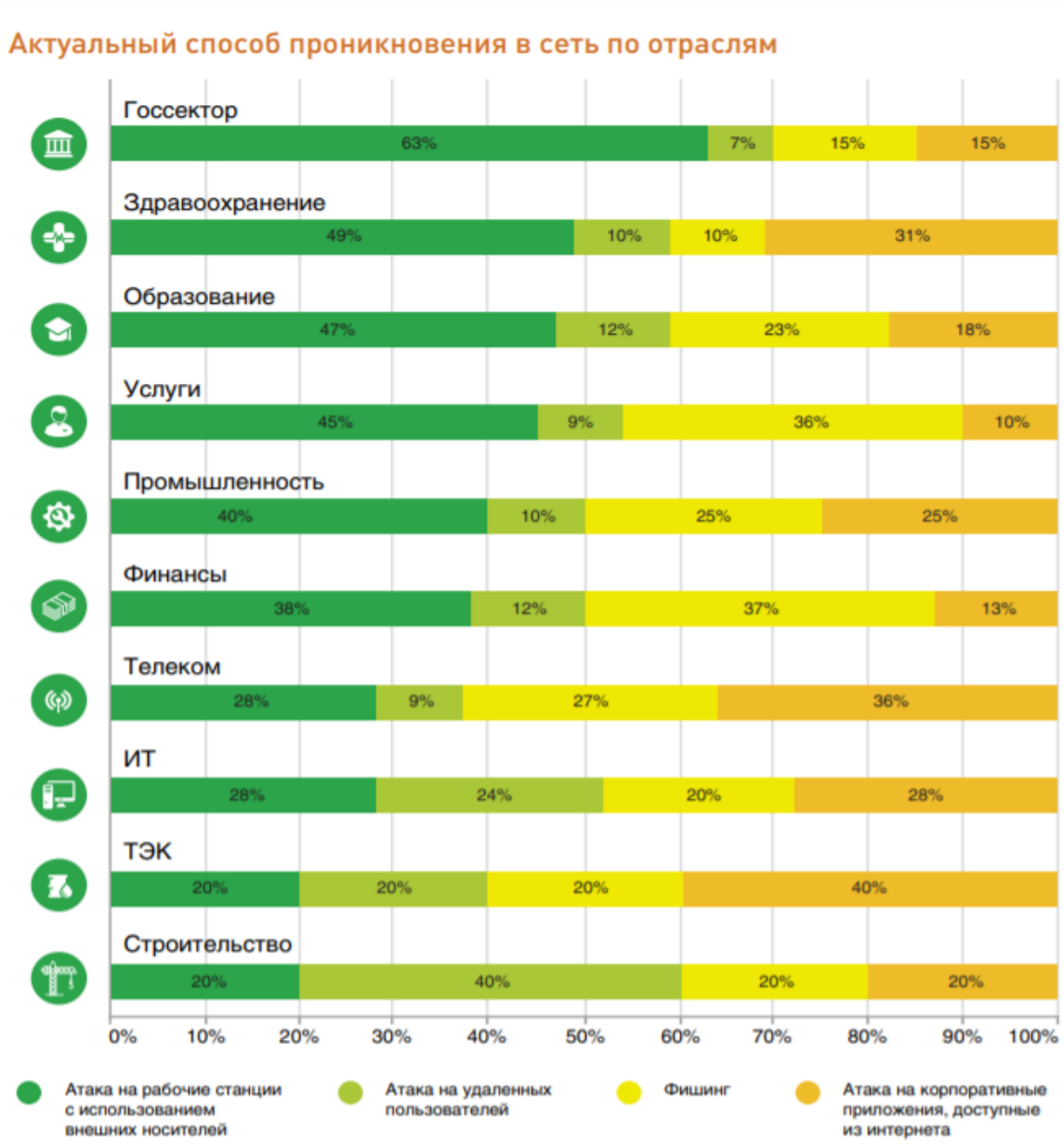


Рис. 1[1]

При этом процесс автоматизации атаки позволяет осуществить перебор уязвимых мест для нахождения точек входа в атакуемую систему. Связано этос с тем, что возрастающая сложность программного и сетевого обеспечения приводит к:

- ошибкам в программном обеспечении, допущенным разработчиком и эксплуатируемым атакующим;
- ошибкам в настройке сетевого и программного обеспечения;
- недостаточной идентификации и аутентификации удаленных компонентов компьютерной сети.

В этих условиях средства защиты не успевают осуществлять выявление атак при динамическом изменении ее этапов [1] (Рис 2).

Рис. 2

Ущерб от нарушения функционирования вычислительных сетей в результате таких деструктивных воздействий со стороны распределенных атак может исчисляться в миллионах и миллиардах рублей. Однако трудности построения защищенных компьютерных систем обусловлена тем, что [1, 2]:

- в среднем российские компании используют решения трех вендоров для обеспечения сетевой безопасности;
- у половины российских компаний нет подразделения, отвечающего за сетевую безопасность;

- удаленный доступ к информационным системам с помощью ноутбуков, планшетов и смартфонов используют 44% крупных компаний;
- менее чем у четверти российских компаний внедрена централизованная система мониторинга ИБ (SIEM);
- на защиту корпоративных сетей компании в среднем выделяют 11% из ИТ-бюджета;
- для оптимизации затрат на построение системы защиты, организации стремятся снизить уровень классификации информационных систем;
- для 76% российских компаний важен вопрос обучения персонала, отвечающего за информационную безопасность.

В этих условиях возникает противоречие как в выборе набора показателей для мониторинга успешности защиты, так и в моделях функционирования компьютерных сетей. Существующие на рынке системы мониторинга и управления не позволяют учитывать динамику изменений стратегий при сетевом взаимодействии, что может привести к снижению устойчивости при отсутствии их согласованности. Таким образом, можно сделать вывод о том, что тема построения защищенных компьютерных сетей весьма актуальна.

Основные элементы многоуровневой системы обеспечения защиты при передаче информации по каналам связи. Принципиальной особенностью межсетевого взаимодействия информационных систем является конвергенция различных каналов, сетей, включенных в технологический процесс обработки информации, сервисов и бизнес-приложений. Сетевые адаптеры, устройства взаимодействия и кабельная система являются тем минимумом оборудования, с помощью которого, возможно создание сетевой инфраструктуры передачи данных (Рис. 3).

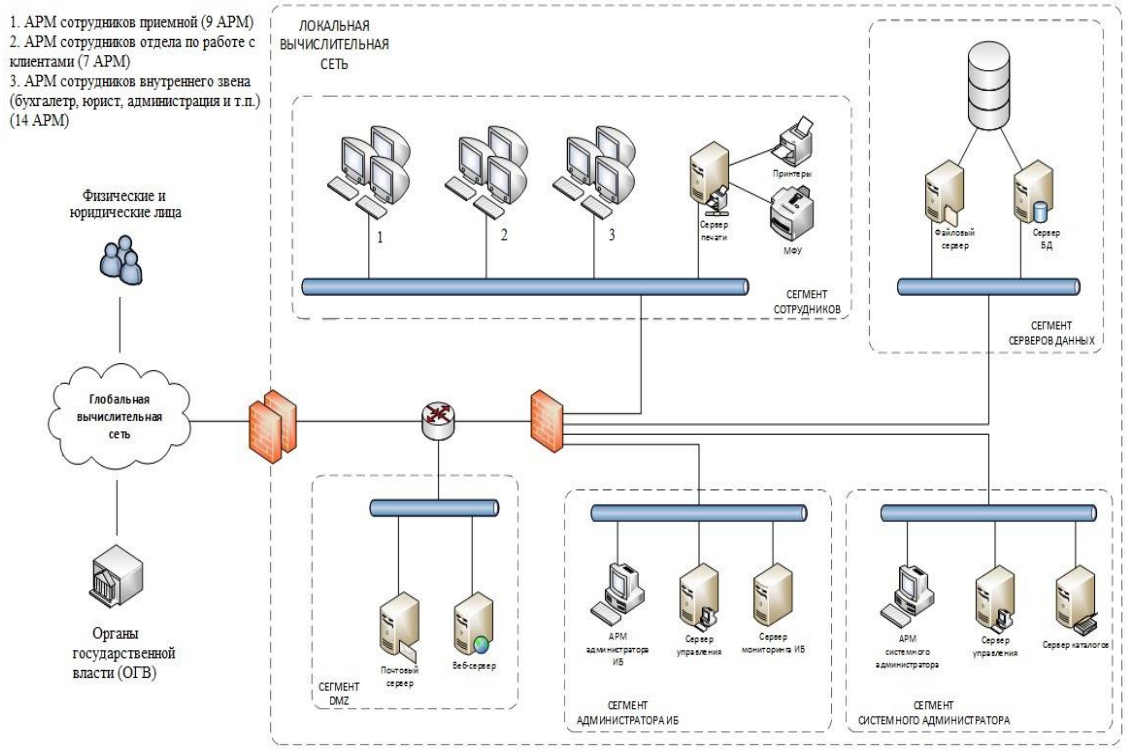


Рис. 3

К основным элементам сетевой инфраструктуры можно отнести:

Платы сетевых адаптеров (сетевые карты) вставляются в слоты расширения всех сетевых компьютеров и серверов, для обеспечения физического соединения между компьютером и сеть и состоит из аппаратной части, а также встроенных программ, записанных в ПЗУ. Эти программы реализуют функции физического и канального уровней модели открытых систем в конечном узле сети и выполняют функции передачи и приема кадра.

Концентраторы относятся к аппаратным средствам физического и канального уровней передачи информации, имеющим несколько портов (выходов), для подключения физического сегмента кабеля, идущего от сетевых адаптеров конечных узлов.

Коммутаторы- устройства, соединяющие 2 и более сети, с одним и тем же протоколом и обрабатывающий кадры параллельно. Каждый из портов коммутатора обслуживается собственным процессором, системным модулем, имеющим общую адресную таблицу и коммутационной матрицей.

Маршрутизаторы-устройства, соединяющее 2 и более сети. использующее одну и более метрик для определения оптимального пути передачи сетевого трафика на основе информации сетевого уровня.

Межсетевые экраны- специализированные комплексы защиты, позволяющие разделять среду передачи на 2 и более части и реализовать набор правил, определяющих условия прохождения пакетов с данными из одной части в другую.

Теоретические основы построения защищенных сетей. Объединение разнородных сетей в единое информационное пространство приводит к тому, что деятельность различных отделов на стыках зон ответственности не всегда отвечает условиям безопасного межсетевого взаимодействия (Рис. 3). Переход к интегрированным сетевым системам существенно отражается на:

- производительности систем передачи данных (в связи с увеличением объема трафика и образованием очередей)
- формировании различных подходов к реагированию на тот или иной инцидент
- применении механизмов регулирования и зон ответственности, что дополнительно влечет нарушения ИБ.

Проблема усугубляется тем, что имеется тенденция к использованию распределенной обработки данных, которая ослабляет эффективность централизованного контроля.

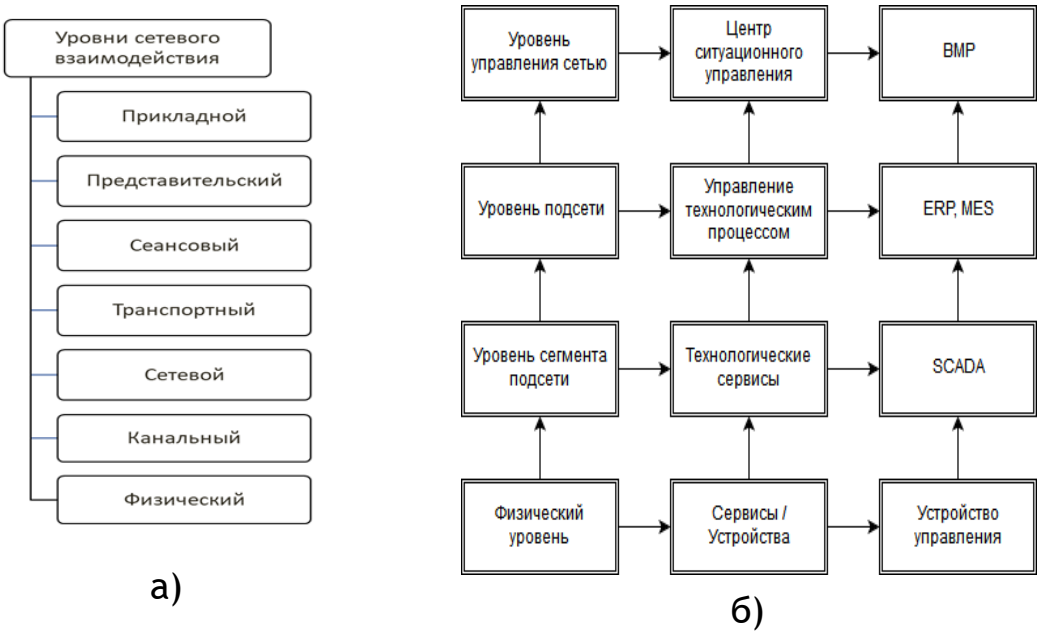
Использование иерархического подхода (Рис. 3) позволяет структурировать потоки информации, облегчить задачу управления безопасностью, а также обеспечить разный уровень защиты информационного потока в зависимости от цели обработки.

Классификация систем обеспечения защиты при передаче информации по каналам связи. В общем случае процессы обработки информации, при которых ее передача происходит по телекоммуникационным каналам, можно представить по:

Уровням сетевого взаимодействия. Использование иерархического подхода позволяет отделять внутренние процессы, протекающие в информационной системе, друг от друга, а также осуществлять контроль за безопасностью передачи данных на каждом из подуровней модели OSI (Рис. 4 а).

Для обеспечения безопасности целесообразно ввести средства защиты на каждом из уровней. Это позволит не только обеспечить защиту, но и

получить оценки, характеризирующие некоторый частный срез оперативной обстановки, в зависимости от поставленных задач. Тогда показатели низких уровней могут измеряться непосредственно на оборудовании, более масштабные – с помощью свёртки низкоуровневых показателей (Рис. 4б).



а) б)

Рис. 4

Использование многоуровневой структуры обеспечения ИБ позволяет осуществлять разделение всего процесса принятия решений на такое число уровней, при котором – решение задачи оптимизации на каждом из них было бы несложным. Однако в случае большого числа подуровней и структурной сложности системы возникает задача согласования и координации решений, принимаемых на всех слоях –управления.

Уровням обеспечения защиты информации. Средства защиты информации в части предотвращения преднамеренных действий в зависимости от способа реализации можно разделить на группы (Рис. 5).

Рис. 5

Формальные средства защиты – выполняют защитные функции строго по заранее предусмотренной процедуре без участия человека. К ним относятся:

Физические- использование технических средств охраны и сооружений, предназначенных для создания физических препятствий на путях проникновения в систему.

Технические- использование технических устройств и программ, входящих в состав ИС и выполняющих функции защиты:

- средства идентификации и аутентификации
- аппаратное шифрование
- управление доступом
- фильтрование трафика

Программные средства - пакеты программ, отдельные программы или их части, используемые для решения задач защиты информации. Программные средства не требуют специальной аппаратуры, однако ведут к снижению производительности, так как требуют выделения под их нужды определенного объема ресурсов и т.п.

Криптографические средства могут использоваться как для защиты обрабатываемой информации в компонентах системы, так и для защиты

информации, передаваемой по каналам связи. Само преобразование информации может осуществляться аппаратными или программными средствами, с помощью механических устройств, вручную и т.д. Неформальные средства защиты – регламентируют деятельность человека.

Правовые и законодательные - действующие в стране законы, указы и другие нормативно-правовые акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее получения, обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей.

Морально-этические -нормы поведения, традиционно сложившиеся в обществе по мере распространения информационных технологий, невыполнение которых приводит к падению авторитета, престижа организации, страны, людей.

Административные или организационные- меры, регламентирующие процессы функционирования компьютерных сетей, деятельность персонала с целью максимального затруднения или исключения реализации угроз безопасности. К данным мерам можно отнести:

- организацию явного или скрытого контроля за работой пользователей
- организацию учета, хранения, использования, уничтожения документов и носителей информации.
- организация охраны и надежного пропускного режима
- мероприятия, осуществляемые при подборе и подготовке персонала
- мероприятия по проектированию, разработке правил доступа к информации
- мероприятия при разработке, модификации технических средств

Основные принципы построения защищенных систем. При построении сетей информации необходимо учитывать ряд принципов:

1. ***Принцип системности*** - системный подход предполагает необходимость учета всех взаимосвязанных и изменяющихся во

времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности.

2. ***Принцип комплексности*** - предполагает построение сетевого взаимодействия из разнородных средств, перекрывающих все существующие каналы реализации угрозы безопасности и не содержащих слабых мест на стыке отдельных компонентов.
3. ***Принцип непрерывной защиты*** - защита должна существовать без разрыва в пространстве и времени. Это непрерывный целенаправленный процесс, предполагающий не только защиту эксплуатации, но и проектирование защиты на стадии планирования системы.
4. ***Принцип разумной достаточности***. Вложение средств в систему защиты должно быть построено таким образом, чтобы получить максимальную отдачу.
5. ***Принцип гибкости управления и применения***. При проектировании системы защита может получиться либо избыточной, либо недостаточной. Система защиты должна быть легко настраиваема.
6. ***Принцип открытости алгоритмов и механизмов защиты***. Знание алгоритма механизма защиты не позволяет осуществить взлом системы.
7. ***Принцип простоты применения защитных мер и средств***. Все механизмы защиты должны быть интуитивно понятны и просты в использовании. Защита информации должна обеспечиваться и при выполнении регламентных и ремонтных работ, во время настройки и

Не следует также забывать, что средства информационной безопасности сами могут представлять собой угрозу сетевому взаимодействию. Для предотвращения такого класса угроз требуют, чтобы алгоритмы и механизмы защиты допускали независимую проверку на безопасность и следование стандартов, а также на возможность их применение в совокупности с другими средствами защиты информации. Рассмотрим классификация методов, используемых для обеспечения информационной безопасности:

- **препятствие** – метод физического преграждения пути злоумышленнику к информации;
- **управление доступом** – метод защиты с помощью регулирования использования информационных ресурсов системы;

- **маскировка** – метод защиты информации путем ее криптографического преобразования;
- **регламентация** – метод защиты информации, создающий условия автоматизированной обработки, при которых возможности несанкционированного доступа сводится к минимуму;
- **принуждение** – метод защиты, при котором персонал вынужден соблюдать правила обработки, передачи и использования информации;
- **побуждение** – метод защиты, при котором пользователь побуждается не нарушать режимы обработки, передачи и использования информации за счет соблюдения этических и моральных норм.

Обеспечение вышеизложенных методов защиты объектов предполагает необходимость выполнения комплекса этапов при построении защищенных систем (рис. 6). Рассмотрим пример обеспечения безопасности сетевых объектов критической информационной инфраструктуры, на примере применения Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Законом определены основные этапы построения защищенных систем, представленных на рис. 6.

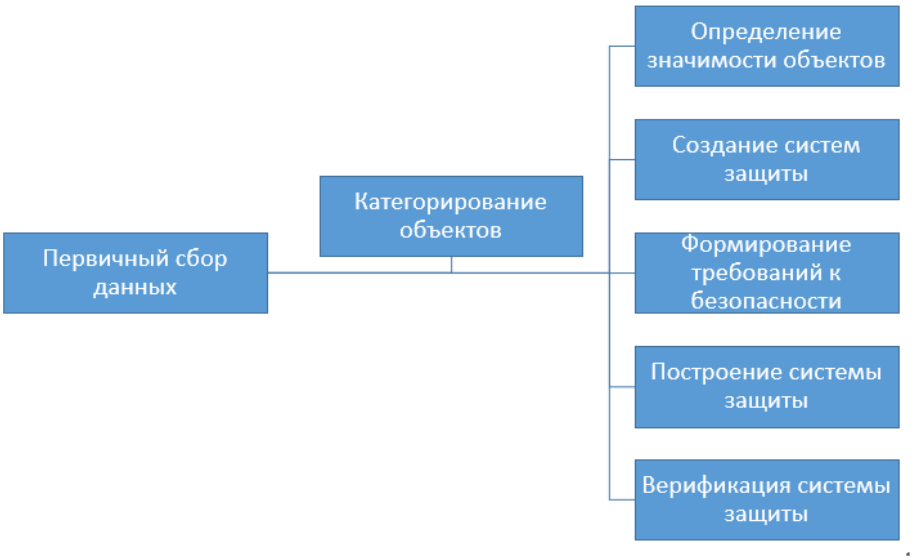


Рис. 6.

Сбор первичных данных о субъекте и объектах. Понятие «субъект критической инфраструктуры» содержится в статье 2 Закона «О безопасности КИИ» и подразумевает:

1. Государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели (далее по тексту – организация):

- функционирующие в одной или нескольких сферах деятельности: здравоохранение, наука, транспорт, связь, энергетика, банковская сфера, сферы финансового рынка, топливно-энергетический комплекс, атомная энергетика, оборонная, ракетно-космическая, горнодобывающая, металлургическая и химическая промышленность;
- которым принадлежат (на праве собственности, аренды, ином законном основании) объекты КИИ.

2. Российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие систем и (или) сетей (ИС, ИТКС, АСУ) принадлежащих субъектам КИИ.

Такое разделение позволяет идентифицировать организацию по учредительным и нормативно-правовым юридическим документам. Например, к таким документам можно отнести: Устав организации; Положение об организации; Единый государственный реестр юридических лиц (ЕГРЮЛ); Единый государственный реестр индивидуальных предпринимателей (ЕГРИП); лицензии и иные разрешительные документы на осуществление конкретных видов деятельности (выполнение работ, оказание услуг), Общероссийский классификатор видов экономической деятельности (ОКВЭД). Для минимизации ошибок целесообразно рассмотреть деятельность организации на каждом уровне ее функционирования (табл 1).

Таблица 1. Пример идентификации критичности отделов организации

	Наименование ИС	ОКВЭД	Критичность объекта
1	Бухгалтерия	69.20.2	+
2	Отдел кадров	52.10.9	-
3	Производство	24.10.1	+

Категорирование объектов ИС, в которой осуществляется циркуляция информации (определения сферы функционирования организации) и

определение сферы функционирования. Следует учитывать, что для конкретной сферы (здравоохранение, наука и т д) будет преобладать один вид системы обработки информации (ИС, АСУТП, ИТКС), поскольку именно он с большей вероятностью будет обрабатывать информацию, необходимую для обеспечения критических процессов, и (или) осуществлять управление, контроль или мониторинг критических процессов.

Таблица 2. Пример классификации объектов КИИ по сфере функционирования

ИС	АСУ	ИТКС
Здравоохранение	Топливно-энергетический комплекс Энергетика	связь
Наука Транспорт	Атомная энергетика	
Банковская сфера	Ракетно-космическая промышленность	

Категорирование объектов. Определение значимости. Категорирование — установление соответствия объекта инфраструктуры критериям значимости и показателям их значений, на основании которых определяется базовый набор степени защищённости.

Проведение процедуры категорирования описано в Постановлении Правительства РФ от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, в соответствие с которой необходимо:

- определить процессы, протекающих в ИС;
- выявить наиболее критические из них, т.е. нарушение которых может привести к негативным последствиям;
- осуществить формирование списка объектов, необходимых для обеспечения функционирования критических процессов и которые подлежат категорированию.

В рамках этих действий осуществляется рассмотрение возможных действий нарушителей в отношении объектов КИИ и анализ угроз безопасности. Это позволяет осуществить оценку объектов ИС в соответствии с показателями значимости и присвоение каждому из объектов ИС категории.

Либо принятие решения об отсутствии необходимости её присвоения (первая, вторая и третья категории) экспертным путем. Частью 3 ст. 7 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» устанавливается три категории значимости объектов критической информационной инфраструктуры - первая, вторая и третья.

Таблица 2. Пример анализа применимости показателей критериев значимости к субъекту КИИ

Показатель	**Значение показателя**		
	III категория	II категория	I категория
Причинение ущерба жизни и здоровью людей (человек)	Более 1, но не менее или равно 50	Более 50, но не менее или равно 500	Более 500

Обеспечение безопасности значимых объектов. Показатели значимости позволяют сформировать перечень СЗИ, которые должны соответствовать категории значимости. Необходимо следить за их адекватностью для противодействия как текущим угрозам, так и угрозам «нулевого дня». Цикл создания и функционирования СОИБ начинается с этапа планирования (рис. 7).

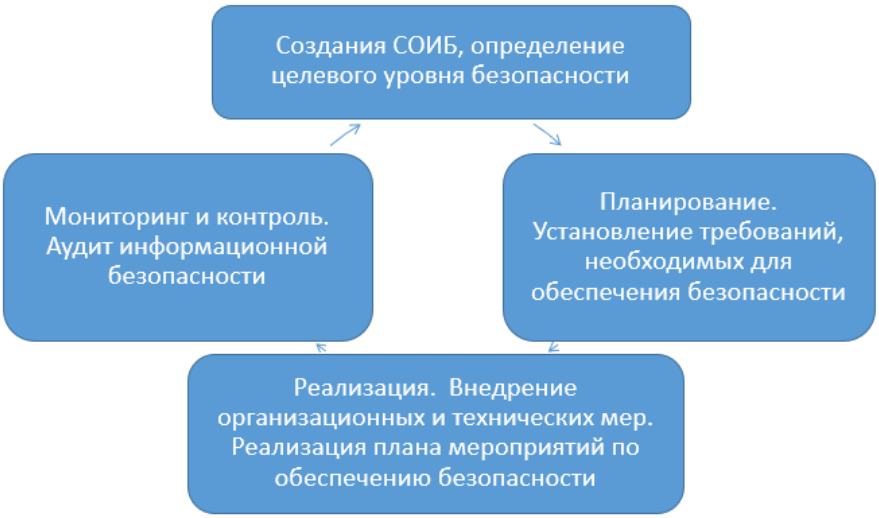


Рис. 7

Планирование. На данном этапе устанавливаются требования, которые необходимо выполнить для обеспечения безопасности и формируется план мероприятий по защите, с учетом требований нормативно-правовой правовой базы [3-12].

Далее осуществляется внедрение организационных и технических мер, реализация плана мероприятий по обеспечению безопасности, в том числе, с учетом [11] и уровней обработки информации (рис 3):

- идентификация и аутентификация;
- управление доступом;
- аудит безопасности;
- антивирусная защита и управление обновлениями программного обеспечения;
- предотвращение вторжений (компьютерных атак) и реагирование на инциденты нарушений информационной безопасности;
- обеспечение целостности и доступности;
- защита технических средств и систем;
- защита информационной (автоматизированной) системы и ее компонентов;
- управление конфигурацией;
- планирование мероприятий по обеспечению безопасности;
- обеспечение действий в нештатных ситуациях;
- информирование и обучение персонала.

К дальнейшим мероприятиям по реализации целесообразно отнести:

1. Проверку готовности СЗИ к использованию, с составлением заключений о возможности эксплуатации СЗИ;
2. Введение в эксплуатацию СЗИ, в соответствии с эксплуатационной и технической документацией;
3. Обучение персонала работе с СЗИ;
4. Учет применяемых СЗИ, эксплуатационной и технической документации к ним;
5. Учет лиц, допущенных к работе с информацией;
6. Формирование нормативно-правовой документации при эксплуатации СЗИ.

Мониторинг и контроль. К мероприятиям по мониторингу и контролю целесообразно отнести:

- проведение процедур, направленных на предотвращение несанкционированного доступа;
- своевременное обнаружение фактов НСД;
- предотвращение воздействий на технические средства обработки информации, в результате которых может быть нарушено их функционирование;
- незамедлительное восстановление информации, которая модифицирована или уничтожена в следствии несанкционированного доступа к ней;
- постоянный мониторинг за обеспечением уровня защищенности.

Ключевым вопросом в рамках контроля состояния безопасности является аудит ИБ, с оценкой эффективности принимаемых организационных и технических мер (рис. 8).

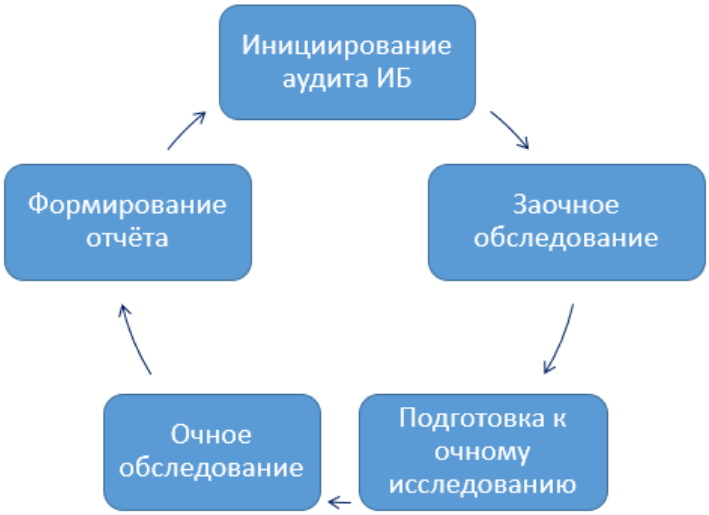


Рис. 8.

В рамках совершенствования безопасности СЗИ целесообразно проводить анализ функционирования системы безопасности и состояния безопасности, по результатам которого разрабатывать предложения по развитию системы безопасности и меры по совершенствованию безопасности.

Литература

1. Исследование российского рынка информационной безопасности. Код безопасности. Электронный ресурс https://www.securitycode.ru/documents/analytics/
2. Как российские компании защищаются от целевых атак. https://www.ptsecurity.com/ru-ru/research/analytics/
3. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
4. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
5. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
6. Указ Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно телекоммуникационных сетей международного информационного обмена».
7. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
8. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
9. Приказ ФСТЭК России от 14.03.2014 № 31 (ред. от 09.08.2018) «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»
10. Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры российской федерации и обеспечению их функционирования»

11. Приказ ФСТЭК России от 25.12.2017 №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры РФ»
12. Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности.