Реализация превентивных мер по нейтрализации актуальных угроз информационной безопасности предприятия связи

Информационная безопасность - это состояние защищённости информационной среды предприятия, полученное в ходе процессов обеспечения конфиденциальности, целостности и доступности информации и передаваемых в рамках выполнения функциональных задач данных.

Защита информации на предприятии представляет собой деятельность ответственных должностных лиц по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть процесс, направленный на достижение этого состояния.

Превентивные меры по нейтрализации актуальных угроз информационной безопасности – это комплекс мероприятий, направленный на предупреждение (недопущение) появления актуальной угрозы. Механизм превентивных средств и методов заключается в выявлении, устранении, локализации, нейтрализации либо минимизации воздействия негативных факторов на защищаемую информацию и ресурсы вычислительной системы, а также в устранении сопутствующих и способствующих реализации замыслов и намерений отдельных лиц и «групп риска».

Актуальные угрозы информационной безопасности

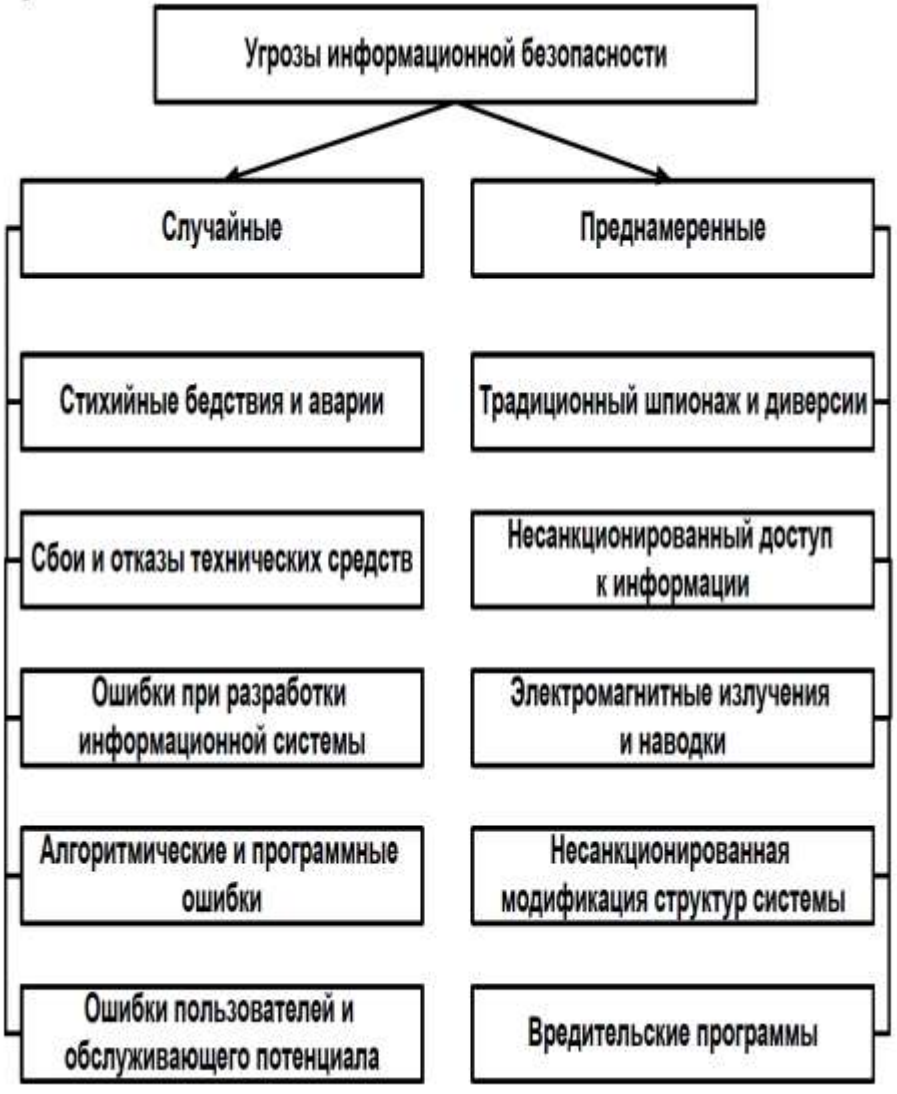
Угрозы безопасности отечественных информационных и телекоммуникационных средств и систем определены в Доктрине информационной безопасности Российской Федерации.

Актуальной считается угроза, которая может быть реализована в информационной системе и представляет опасность для информации ограниченного доступа.

Угрозы безопасности информации определяются по результатам:

•оценки возможностей внешних и внутренних нарушителей (потенциала, оснащенности и мотивации);
•анализа возможных уязвимостей ИС;
•анализа возможных способов реализации угроз безопасности информации;
•анализа последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

Общий перечень угроз ИБ



В информационных системах предприятий, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена, возможна реализация следующих угроз безопасности:

- угрозы утечки информации по техническим каналам;
- угрозы несанкционированного доступа к информации;
- угрозы из внешних сетей.
- Угрозы из внешних сетей включают в себя:
- угрозы «анализа сетевого трафика»;
- угрозы сканирования;
- угрозы выявления паролей;
- угрозы получения несанкционированного доступа путем подмены доверенного объекта;
- угрозы типа «отказ в обслуживании»;
- угрозы удаленного запуска приложений;
- угрозы внедрения вредоносных программ.

Перечень необходимых и оперативных мер защиты информации определяется по результатам проверки информационной безопасности информационной системы и анализа рисков с учетом соотношения затрат на защиту информации с возможным ущербом от ее разглашения, утраты, уничтожения, искажения, нарушения доступности информации и работоспособности программно-технических средств, обрабатывающих эту информацию.

Предупреждение возможных угроз и противоправных действий может быть обеспечено самыми различными мерами и средствами, начиная от создания климата глубоко осознанного отношения сотрудников к проблеме безопасности и защиты информации до создания глубокой, эшелонированной системы защиты физическими, аппаратными, программными и криптографическими средствами. Предупреждение угроз возможно и путем получения информации о готовящихся противоправных актах, планируемых хищениях, подготовительных действиях и других элементах преступных деяний.

В предупреждении угроз весьма существенную роль играет информационно-аналитическая деятельность службы безопасности на основе глубокого анализа криминогенной обстановки и деятельности конкурентов и злоумышленников.

Организационные, правовые и экономические методы защиты информации в информационной системе стоят на первом месте в технологиях предотвращения угроз информационной безопасности.

Организационные методы защиты информации включают в себя меры, мероприятия и действия, которые должны осуществлять должностные лица в процессе создания и эксплуатации информационной системы для обеспечения заданного уровня безопасности обработки информации.

Правовые методы защиты информации основываются на законодательной базе обеспечения информационной безопасности .

Экономические методы включают:

- разработку программ обеспечения информационной безопасности и определение порядка их финансирования;
- совершенствование системы финансирование работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.

Состав превентивных мер противодействия угрозам, характерным для АС предприятий связи

Актуальные угрозы ИБ	Превентивные меры по нейтрализации угроз
Угрозы, связанные с применением технических средств автоматизации	
Физическое повреждение аппаратных средств	обеспечение охраны аппаратных средств; обеспечение адекватного резерва критичных аппаратных средств; обеспечение периодического копирования информации.
Физическое повреждение линий связи	дублирование линий связи; наличие альтернативных линий связи; обеспечение охраны линий связи.
Перебои в системе электропитания	использование блоков бесперебойного питания; использование резервного автономного источника питания.
Отказы аппаратных средств	“горячее” и “холодное” резервирование аппаратных средств; регулярное проведение регламентных работ; наличие соответствующих средств диагностики; ежедневное тестирование аппаратных средств.

Состав превентивных мер противодействия угрозам, характерным для АС предприятий связи

Установка непроверенных аппаратных средств или замена вышедших из строя аппаратных компонент системы на не идентичные компоненты	организационно-технические мероприятия, направленные на регламентирование процедур включения, замены и модификации технических средств в системе, а также при их закупке, проверке работоспособности, хранении на складе.
Отсутствие контроля за снятыми с системы (не уничтоженными) вышедшими из строя запоминающими устройствами с записанной на них конфиденциальной информацией	регламентация хранения, списания и уничтожения носителей информации, содержащих критичную информацию; хранение ключевой и прикладной информации в защищенном (зашифрованном) виде.

Состав превентивных мер противодействия угрозам, характерным для АС предприятий связи

Угрозы, связанные с использованием программного обеспечения	
Ошибки в программном обеспечении	тестирование программного обеспечения разработчиками; тестирование программного обеспечения независимыми экспертами; наличие периода опытной эксплуатации системы; сертификация программного обеспечения на соответствие техническим условиям и на отсутствие недекларированных возможностей; получение и хранение эталонных исходных текстов и загрузочных модулей; получение и хранение конструкторской и эксплуатационной документации на программное изделие; регламентирование процедур ввода в эксплуатацию, модификации и замены программного обеспечения в действующую систему; контроль целостности файлов; отслеживание выхода новых "патчей" и обновление программного обеспечения.

Состав превентивных мер противодействия угрозам, характерным для АС предприятий связи

Анализ и модификация программного обеспечения	контроль целостности системы; ограничение доступа к репозиторию программного обеспечения (исходным текстам программ и загрузочным модулям); контроль несанкционированного доступа; удаление из действующей системы всех средств отладки и любых других программ, которые могут использоваться как инструментарий для анализа программного обеспечения; разделение вычислительных сетей, предназначенных для разработки программного обеспечения и сетей действующей автоматизированной системы; регламентация установки, модификации и замены программного обеспечения в действующей автоматизированной системы; анализ журналов регистрации.
Наличие в программном обеспечении “закладок” и “троянских коней”	контроль целостности системы; проверка благонадежности программистов-разработчиков; организация надлежащего хранения и контроля допуска к исходным текстам программ, средствам программирования и отладки; тестирование программного обеспечения независимыми экспертами; проведение опытной эксплуатации, сертификация программного обеспечения на соответствие техническим условиям и на отсутствие недекларированных возможностей; постоянный антивирусный контроль; использование сканеров безопасности; закрытие лишних портов; анализ журналов регистрации.

Состав превентивных мер противодействия угрозам, характерным для АС предприятий связи

Атаки программных вирусов	создание закрытой среды функционирования программного обеспечения системы; контроль целостности программного обеспечения; контроль наличия неизвестных программ; контроль доступа к системе; регулярное тестирование программного обеспечения антивирусными программами; использование лицензионного программного обеспечения.
Угрозы, связанные с нарушением технологического процесса обмена данными	
Отказ от авторства сообщения (отказ от факта получения сообщения, подмена принятого сообщения, имитация принятого сообщения, подмена передаваемого сообщения, имитация передаваемого сообщения, нарушение целостности потока сообщений)	аутентификация пользователей и электронных сообщений; использование криптографических механизмов электронной цифровой подписи, шифрование сообщения; регистрация и архивация входящих и исходящих сообщений; использование механизмов автоматического квитирования получения сообщений и документов; закрытие системы от использования внешних программ, позволяющих модифицировать полученные сообщения; создание группы разбора конфликтных ситуаций и регламентация процедуры установления и доказательства авторства; организация нумерации сообщений и контроль непрерывности номеров; регистрация и архивация входящих и исходящих сообщений.

Состав превентивных мер противодействия угрозам, характерным для АС предприятий связи

Угрозы безопасности со стороны персонала	
Несанкционированное получение и использование привилегий	контроль несанкционированного доступа; активный аудит; регистрация всех действий пользователей; анализ журналов регистрации работы системы; контроль сотрудниками службы безопасности соответствия установленных полномочий и их использования; закрепление за разными категориями пользователей конкретных рабочих мест; строгая регламентация функций назначения, внесения и изменения полномочий.
Прерывание процесса передачи и обработки информации	“горячее” и “холодное” резервирование технических средств и каналов связи; реализация возможности автоотката для восстановления вычислительного процесса; дублирование входящей в систему информации и результатов промежуточных расчетов.
Разглашение реализации программной защиты	организация надлежащего хранения и доступа к технической документации и программным средствам защиты; периодическое изменение паролей и ключей.
Раскрытие, перехват, хищение кодов, ключей, паролей	контроль несанкционированного доступа; аутентификация; анализ журналов регистрации.

Состав превентивных мер противодействия угрозам, характерным для АС предприятий связи

Чтение остаточной информации в оперативной памяти и на магнитных носителях	ограничение доступа по работе с техническими средствами и магнитными носителями; ограничения на использование программных средств, не входящих в состав системы; регистрация и контроль действий пользователей при работе в системе.
Ошибочный ввод данных	автоматический контроль ввода критичных данных; необходимость подтверждения ввода тех параметров сообщений, которые значительно отличаются от среднестатистических или не попадают в список разрешенных значений или разрешенный диапазон.
Умышленная порча аппаратного и программного обеспечения	организация пропускного режима, видеонаблюдения и охраны доступа к системе; организация работы обслуживающего персонала по наблюдению за правильным использованием программных и технических средств.
Хищение носителей информации, производственных отходов	организация пропускного режима и охраны системы; регламентация учета, хранения и выдачи носителей информации.

Состав превентивных мер противодействия угрозам, характерным для АС предприятий связи

Угрозы, связанные с попытками "взлома" системы безопасности	
Взлом программной защиты	ограничение доступа к технической и эксплуатационной документации на средства защиты информации; использование административных мер защиты; постоянное совершенствование и модификация средств защиты; ограничение количества попыток подключения к системе при неправильном вводе пароля; регистрация “неудачных” попыток подключения к системе и анализ регистрационных журналов; постоянный контроль и анализ работы системы защиты; периодическое изменение паролей и ключей.
Наблюдение за работой системы	ограничение доступа к системе; ограничение на использование программ, не входящих в состав системы; административные меры защиты.
Использование сетевых анализаторов	административные меры защиты; использование сканеров безопасности; использование средств отражения атак в реальном масштабе времени; использование закрытого трафика сети; шифрование передаваемой информации; использование межсетевых экранов.
Перехват информации на линиях связи	шифрование передаваемой информации.

Состав превентивных мер противодействия угрозам, характерным для АС предприятий связи

Угрозы, связанные с естественными и природными факторами	
Пожар и другие стихийные бедствия	организация противопожарной защиты; обучение персонала действиям в чрезвычайных ситуациях.
Кража оборудования	организация охраны объектов; установка специального оборудования; административные меры.
Диверсии	организация пропускного режима и охраны объектов; установка систем контроля проноса на объекты оружия, взрывчатых, химических, биологических, отравляющих и радиационных веществ; административные меры.

Реализация превентивных мер по нейтрализации актуальных угроз

Для реализации превентивных мер на предприятиях связи проводятся следующие организационные и технические мероприятия:

•издание приказа о назначении структурного подразделения или должностного лица (работника), ответственного за обеспечение безопасности информации;

•разработка документов, регламентирующих политику в отношении обработки информации;

•организация общей подготовки кадров организаций и предприятий для выполнения установленных требований по обеспечению информационной безопасности;

•организация подготовки специалистов для эксплуатации систем и средств защиты и обеспечения контроля соблюдения установленных требований к информационной безопасности в деятельности организаций, предприятий;

•определение правил реагирования сотрудников на события, несущие угрозу безопасности;

•вменение в обязанности сотрудникам обязательное уведомление об обнаруженных инцидентах и слабых местах в системе безопасности;

•определение ответственности за нарушение режима безопасности информации;

•разработка процедуры оценки вреда (ущерба), который может быть причинен собственнику информации в случае нарушения действующего законодательства Российской Федерации;

Реализация превентивных мер по нейтрализации актуальных угроз

- организация процедуры определения угроз безопасности информации при их обработке и формирования на их основе модели угроз;
- организация процедуры проведения классификации информационных систем;
- определение границы контролируемой зоны и фиксация в приказе по организации;
- организация процедуры установки и ввода в эксплуатацию средств защиты информации;
- организация процедуры проверки готовности средств защиты информации к использованию;
- организация процедуры оценки эффективности принимаемых мер по обеспечению безопасности информации до ввода в эксплуатацию информационной системы;
- разработка инструкции регламентирующей использование средства защиты информации в соответствии с правилами пользования этими средствами;
- организация процедуры ознакомления работников, непосредственно осуществляющих обработку информации, с требованиями законодательных и нормативных актов под роспись;
- организация процедур контроля за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

Реализация превентивных мер по нейтрализации актуальных угроз

- организация процедуры учета применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей конфиденциальных данных;
- установление правил доступа к информации;
- организация процедуры регистрации и учета всех действий, совершаемых с конфиденциальными данными в информационной системе;
- организация процедуры периодической проверки электронного журнала обращений должностными лицами;
- организация учета лиц, допущенных к работе с информацией в информационной системе;
- организация учета машинных носителей информации;
- организация процедуры восстановления информации, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- организация процедуры контроля за принимаемыми мерами по обеспечению безопасности информации и уровня защищенности информационных систем;
- организация процедуры периодического внутреннего контроля и (или) аудита соответствия обработки информации требованиям законодательных и нормативных актов;
- организация процедуры проведения разбирательств по фактам несоблюдения условий хранения носителей данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности данных или другим нарушениям, приводящим к снижению уровня защищенности данных;

- размещение устройств ввода/вывода информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав информационной системы, в помещениях, таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации;
- должна быть организована охрана помещений, в которых размещены информационные системы, в которых ведется работа с информацией;
- должна обеспечиваться сохранность носителей конфиденциальной информации и средств защиты информации, исключаться возможность неконтролируемого проникновения или пребывания посторонних лиц в помещения с АРМ ИС;
- должна быть разработана организационная и распорядительная документация, регламентирующая организацию физической защиты помещений и технических средств, размещение технических средств в пределах охраняемой территории, ограничение доступа пользователей в помещения, где размещены технические средства, а также хранятся носители информации, реализацию разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, установление правил доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации, управление доступом к защищаемым данным, регистрацию и учет действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

- технические (аппаратные) средства ИС должны быть подключены к системе электропитания и заземления в соответствии с «Правилами устройства электроустановок (ПУЭ)»;
- в составе ИС должны применятся технические (аппаратные) средства, соответствующие требованиям стандартов Российской Федерации по электромагнитной совместимости, безопасности и санитарным нормам или прошедшие специальные исследования установленным порядком и имеющим предписание на эксплуатацию;
- должны выполняться требования предписания на эксплуатацию;
- понижающие трансформаторные подстанции электропитания и контуры заземления технических средств должны быть размещены в пределах контролируемой зоны;
- должна обеспечиваться развязка цепей электропитания, линий связи технических средств;
- использование сертифицированных средств защиты информации;
- помещения, в которых установлены АРМ ИС имеющие в своем составе средства голосового ввода, защищаемые помещения (ЗП) должны размещаться в пределах контролируемой зоны на максимальном удалении от ее границ, ограждающие конструкции помещения (стены, полы, потолки) не должны являться смежными с помещениями других организаций;
- окна помещений должны закрываться шторами (жалюзи);

Реализация превентивных мер по нейтрализации актуальных угроз

- защищаемые помещения должны быть оснащены сертифицированными по требованиям безопасности информации или прошедшими специальные исследования и имеющие предписание на эксплуатацию ОТСС и ВТСС;
- использовать сертифицированные по требованиям безопасности информации или прошедшие специальные исследования и имеющие предписание на эксплуатацию АТС;
- обеспечить уровень звукоизоляции (виброизоляции) ограждающих конструкции ЗП не ниже приведенных в методических документах ФСТЭК России;
- применение сертифицированных средств защиты от НСД;
- использование защищенных каналов связи, применение сертифицированных СКЗИ;
- применение сертифицированных межсетевых экранов;
- резервирование технических средств, дублирование массивов и носителей информации;
- предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок, использование сертифицированных антивирусных средств;
- применение средств анализа защищенности;
- применение средств обнаружения вторжений;
- локализация и сегментация ИС;
- применение сертифицированных средств защиты среды виртуализации;
- контроль разработчиков (поставщиков) программного обеспечения как резидентов Российской Федерации.

- специальное тестирование программных средств;
- персональная ответственность разработчиков за возможные негативные последствия, связанные с несоответствием функциональных характеристик приобретаемого программного обеспечения заявленным требованиям;
- обязанность поставщика по поддержке поставляемого программного обеспечения;
- создание репозиториев для хранения исходных текстов и дистрибутивов программного обеспечения, обеспечивающих необходимую поддержку программного обеспечения.

Реализация превентивных мер защиты должна осуществляться на основе утвержденных конкретных программ и планов, которые ежегодно уточняются с учетом:

- федерального законодательства и нормативной базы в области защиты информации;
- международных и отраслевых стандартов в области информационной безопасности и IT-безопасности;
- организационно-распорядительных документов организации;
- реальных потребностей в средствах обеспечения информационной безопасности;
- объемов финансирования, выделяемых на обеспечение информационной безопасности организации.

Заключительные положения

Организация работ по защите информации должна возлагаться на руководителя организации – владельца информационной системы и руководителей функциональных подразделений организации, эксплуатирующих объекты информатизации, а методическое руководство и контроль за обеспечением защиты информации - на руководителя подразделения по защите информации в организации.

Порядок организации на предприятии работ по созданию и эксплуатации информационной системы должен определяться в соответствующем нормативном документе организации. Данный документ должен определять:

подразделения и отдельных специалистов, в т.ч. специализированных организаций, участвующих в разработке и эксплуатации информационной системы, их задачи и функции на различных стадиях создания и эксплуатации;

вопросы взаимодействия всех занятых в этой работе функциональных подразделений организации и специалистов;

ответственность должностных лиц за качество и научно-технический уровень, за своевременность и качество постановки требований по защите информации.

Документ должен определять стратегию организации в области информационной безопасности, а также ту меру внимания и количество ресурсов, которую руководство считает целесообразным выделить.

Спасибо за внимание!