Акционерное общество
«Корпорация космических систем специального назначения
«Комета»
(АО «Корпорация «Комета»)

Комплексная система обеспечения информационной безопасности в АО «Корпорация «Комета»

Основное понятие информационная безопасность

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ – сохранение

- **Конфиденциальной информации**
- **Целостности информации**
- **Доступности информации**

Конфиденциальность – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право, а также не предоставлять такую информацию третьем лицам без согласия ее обладателя.

Целостность – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Доступность – состояние информации, при котором субъекты, имеющие право доступа, могут реализовать их беспрепятственно.

Виды информации

ИНФОРМАЦИЯ

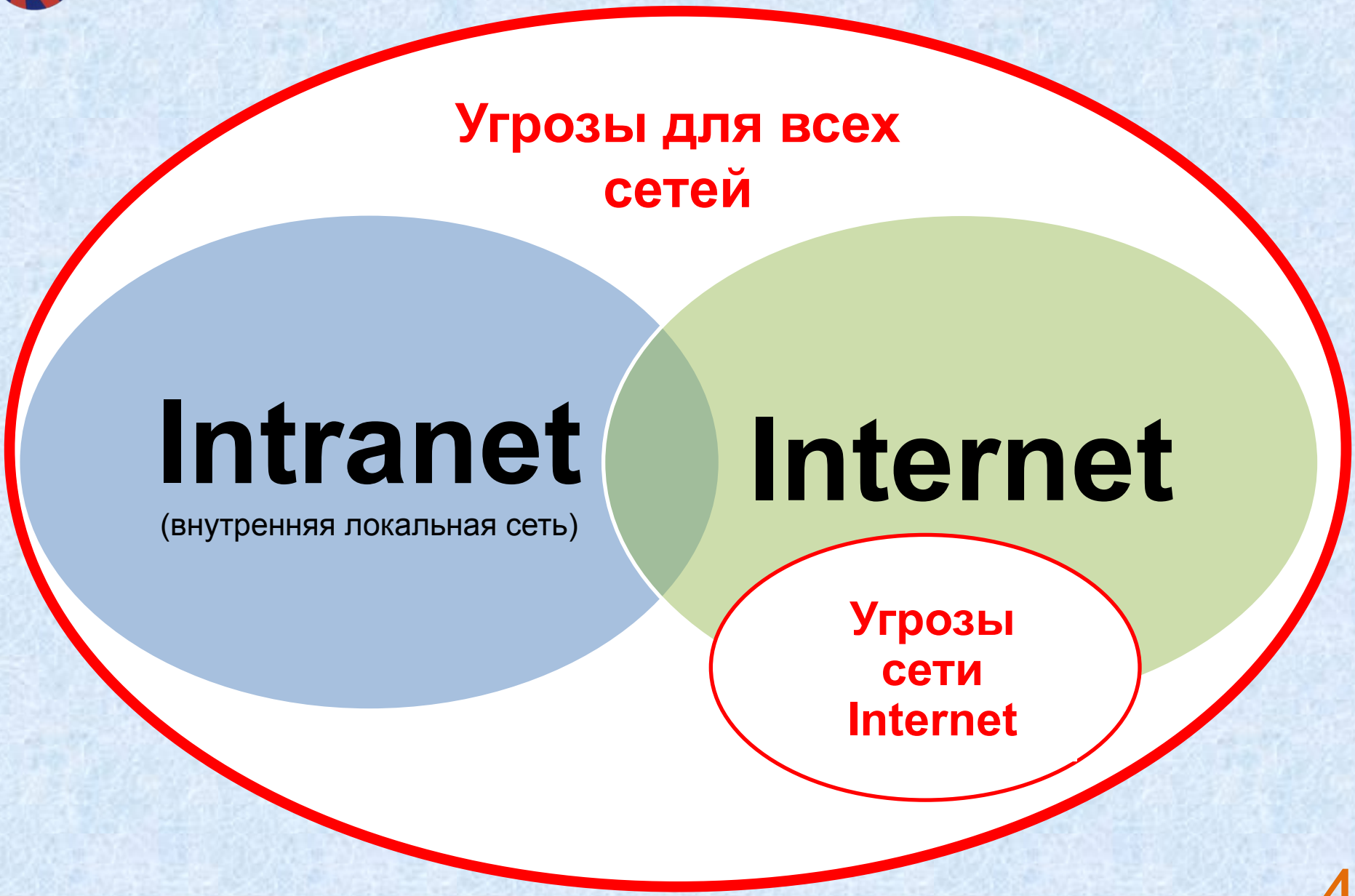
Общедоступная информация

Информация ограниченного доступа

Информация, составляющая государственную тайну

Иная конфиденциальная информация

Угрозы информационным сетям



Детализация угроз информационным сетям

Угрозы для всех сетей (Общие)

1. Заражение вредоносным программным обеспечением
2. Распространение вредоносного программного обеспечения
3. Успешная эксплуатация уязвимости
4. Несанкционированный доступ в систему
5. Сбор сведений с использованием информационно-коммуникационных технологий
6. Компрометация учетной записи администратора и пользователя
7. Несанкционированное использование не учтенных съемных носителей информации
8. Несанкционированный вывод серверного оборудования из строя
9. Несанкционированное разглашение информации
10. Утечка конфиденциальной информации

Угрозы сети Internet

1. Прослушивание сетевого трафика
2. Социальная инженерия, направленная на компрометацию
3. Компьютерная атака типа отказ в обслуживании

Угрозы ИС, являющимся объектами КИИ

Использование неучтенных съемных носителей информации

Компрометация учетных записей администратора и пользователя

Распространение вредоносного ПО

Успешная эксплуатация уязвимости

Заражение вредоносным ПО

Утечка конфиденциальной информации

Разглашение информации

Вывод серверного оборудования из строя

НСД

Сбор сведений с использованием ИКТ

Информационные системы*

Последствия

Вымогательство денежных средств за восстановление доступа к служебной информации

Неконтролируемое движении денежных средств, в т.ч. в части исполнения ГОЗ

Невозможность исполнения обязательств перед контрагентам

Невыплата ЗП

Административная и уголовная ответственность

* ИС - АСУБП, КИС ФЛАГМАН, 1С: Управление холдингом, 1С: УПП, ИСКУ,

Угрозы ИТС, являющимся объектами КИИ

Угрозы АСУ ТП, являющимся объектами КИИ

Перечень средств защиты информации применяемых в локальной вычислительной сети «Интернет»

№	Наименование средства защиты информации	Количество средств защиты информации (шт.)	Тип средства защиты информации	Подсистема СЗИ
1	КриптоПро CSP версия 5.0	70	Средство криптографической защиты информации	- Подсистема защиты электронной подписи и применение электронных подписей в государственных и негосударственных информационных системах
2	Лицензия на право использования СКЗИ «КриптоАРМ» версии 5	6		
3	Средство защиты информации «Secret Net Studio 8»	130	- Средство защиты информации от несанкционированного доступа - Средство контроля подключения съемных машинных носителей информации	- Подсистема идентификации и аутентификации - Подсистема управления доступом - Подсистема ограничения программной среды - Подсистема защиты машинных носителей информации - Подсистема регистрации событий безопасности - Подсистема обеспечения целостности
4	Программно-аппаратный комплекс «Соболь». Версия 4, PCIe и M.2	86	Средство доверенной загрузки операционной системы	Подсистема управления доступом
5	Dr.Web Desktop Security Suite	200	Средство антивирусной защиты	Подсистема антивирусной защиты информации от троянов, шифровальщиков, вирусов и т.д.
6	Dr.Web Server Security Suite	5		
7	Dr.Web Mail Security Suite	1000		
8	КИБ СёрчИнформ в полном составе без дополнительных модулей (ProfileCenter, FileAuditor и DatabaseMonitor)	95	Средство обнаружения утечек конфиденциальной информации	Подсистема защиты конфиденциальной информации
9	vGate R2 Standard	1	Средство защиты платформ виртуализации	Подсистема защиты виртуальной инфраструктуры
10	UserGate 6.6	5	Средство межсетевого экрана	Подсистема межсетевого экранирования
11	Континент СОА	6	Средство обнаружение компьютерных атак	Подсистема обнаружения вторжений

Перечень средств защиты информации применяемых во внутренней локальной вычислительной сети Общества и

№	Наименование средства защиты информации	Количество средств защиты информации (шт.)	Тип средства защиты информации	Подсистема СЗИ
1	Аппаратно-программный комплекс шифрования «Континент» 3.9. Отказоустойчивый (НА) кластер	14	Средство криптографической защиты информации	- Подсистема регистрации событий безопасности - Подсистема защиты информационной системы, ее средств, систем связи и передачи данных по открытым каналам связи
2	КриптоПро CSP версия 5.0	1		- Подсистема защиты электронной подписи и применение электронных подписей
3	Лицензия на право использования СКЗИ «КриптоАРМ» версии 5	1		Подсистема подписания документов электронной подписью
4	Средство защиты информации «Secret Net Studio 8»	2144	- Средство защиты информации от несанкционированного доступа - Средство межсетевого экранирования - Средство контроля подключения съемных машинных носителей информации	- Подсистема идентификации и аутентификации - Подсистема управления доступом - подсистема ограничения программной среды - Подсистема защиты машинных носителей информации - Подсистема регистрации событий безопасности - Подсистема обеспечения целостности
5	Dr.Web Desktop Security Suite	2174	Средство антивирусной защиты	Подсистема антивирусной защиты информации от троянов, шифровальщиков, вирусов и т.д.
6	Dr.Web Server Security Suite	54		
7	vGate R2 Standard	14	Средство защиты платформ виртуализации	Подсистема защиты виртуальной инфраструктуры

Организационно-технические меры в области информационной

Организационные меры

1. Разработка Концепции информационной безопасности
2. Разработка Политики информационной безопасности
3. Разработка политик в рамках Концепции и Политики информационной безопасности
4. Разработка регламентов, положений, инструкций, памяток и т.д.

Технические меры

Использование сертифицированных средств защиты информации:

1. **Средство анализа защищенности и уязвимости**
2. **Система глубокого анализа сетевого трафика**
3. **Замкнутая среда предварительного выполнения программ («песочница»)**
4. **Средство управления информацией об угрозах безопасности информации**
5. **Средство мониторинга информационной безопасности**
6. **Система для защиты критической информационной инфраструктуры**
7. **Средство обнаружения утечек конфиденциальной информации**
8. **Система гарантированного уничтожения информации**
9. **Система для автоматизации действий по реагированию на инциденты**
10. **Средства защиты платформ виртуализации**

Перечень потребности в области информационной безопасности на 2023 год для АО «Корпорация «Комета» и филиалов

Для обеспечения выполнения требований информационной безопасности в локальных вычислительных сетях «Интранет» и «Интернет» Общества и филиалов, необходимо осуществить закупку программно-аппаратных комплексов и программного обеспечения на 2023 год. Перечень потребности на 2023 год представлен отдельным документом.

Ответственность

Создание, распространение и (или) использование ПО, предназначенного для неправомерного воздействия на КИИ

Неправомерный доступ к охраняемой информации, содержащейся в КИИ

Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой информации, содержащейся в КИИ

Лишение свободы на срок от двух до пяти лет со штрафом

Лишение свободы на срок от двух до шести лет со штрафом

Злоумышленник

Принудительные работы на срок до 5 лет с лишением права занимать определенные должности на срок до 3 лет, либо лишение свободы на срок до 6 лет с лишением права занимать определенные должности на срок до 3 лет

Субъект КИИ

Статья 274.1 УК РФ Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации