# СУЩНОСТЬ И ПОНЯТИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ИБ).

# МЕСТО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СТРАНЫ.

**Опр.1 Безопасность информационных ресурсов (информации) - это защищенность информации во времени и пространстве от любых объективных и субъективных угроз, возникающих в обычных условиях функционирования организации и условиях экстремальных ситуаций.**

# Угрозы:

стихийные бедствия, другие неуправляемые события, пассивные и активные попытки злоумышленников создать потенциальную или реальную угрозу несанкционированного доступа к документам, делам, базам данных.

**Опр. 2 ИБ — это комплекс мероприятий, обеспечивающий следующие факторы:**

- конфиденциальность — возможность ознакомиться с информацией (с данными или сведениями, несущими смысловую нагрузку, а не с последовательностью бит их представляющих) имеют в своем распоряжении только те лица, кто владеет соответствующими полномочиями;

- **целостность** — возможность внести изменение в информацию (смысловое выражение) должны иметь только те лица, кто на это уполномочен;

- **доступность — возможность получения авторизованного доступа к информации со стороны уполномоченных лиц в соответствующий санкционированный для работы период времени.**

# Дополнительные факторы:

- учет, т. е. все действия лица, выполняемые им в рамках, контролируемых системой безопасности, должны быть зафиксированы и проанализированы;

- неотрекаемость или апеллируемость т. е. лицо, направившее информацию другому лицу, не может отречься от факта направления информации, а лицо, получившее информацию, не может отречься от факта ее получения.
- Чем это может быть обеспечено?

- *Учет* обычно ведется средствами *электронных регистрационных журналов*, которые используются в основном только уполномоченными службами, и его основное отличие — в регулярности анализа этих журналов.

- *Апеллируемость* обеспечивается средствами *криптографии* (электронно-цифровой подписью), и ее характерная черта — возможность использования в качестве доказательного материала во внешних инстанциях, например в суде, при наличии соответствующего законодательства.

# Механизмы информационной безопасности (ИБ)

# 1) политика

— набор формальных (официально утвержденных либо традиционно сложившихся) правил, которые регламентируют функционирование механизма ИБ;

# 2) идентификация

— определение (распознавание) каждого участника процесса информационного взаимодействия перед тем как к нему будут применены какие бы то ни было понятия ИБ;

# 3) аутентификация

— обеспечение уверенности в том, что участник процесса обмена информацией идентифицирован верно, т. е. действительно является тем, чей идентификатор он предъявил;

# 4) контроль доступа

— создание и поддержание набора правил, определяющих каждому участнику процесса информационного обмена разрешение на доступ к ресурсам и уровень этого доступа;

# 5) авторизация

— формирование профиля прав для конкретного участника процесса информационного обмена (аутентифицированного или анонимного) из набора правил контроля доступа;

# 6) аудит и мониторинг

— регулярное отслеживание событий, происходящих в процессе обмена информацией, с регистрацией и анализом значимых или подозрительных событий;

Понятия "аудит" и "мониторинг" при этом несколько различаются, так как первое предполагает анализ событий постфактум, а второе приближено к режиму реального времени

# 7) реагирование на инциденты

— совокупность процедур или мероприятий, которые производятся при нарушении или подозрении на нарушение ИБ;

# 8) управление конфигурацией

— создание и поддержание функционирования среды информационного обмена в работоспособном состоянии и в соответствии с требованиями ИБ;

# 9) управление пользователями

— обеспечение условий работы пользователей в среде информационного обмена в соответствии с требованиями ИБ;

**В данном случае под пользователями понимаются все, кто использует данную информационную среду, в том числе и администраторы**

# 10) управление рисками

— обеспечение соответствия возможных потерь от нарушения ИБ мощности защитных средств (то есть затратам на их построение);

# 11) обеспечение устойчивости

— поддержание среды информационного обмена в работоспособном состоянии и соответствии требованиям ИБ в условиях деструктивных внешних или внутренних воздействий.

# Инструментарий информационной безопасности

# 1) персонал

— люди, которые будут обеспечивать претворение в жизнь ИБ во всех аспектах, то есть разрабатывать, внедрять, поддерживать, контролировать и исполнять;

# 2) нормативное обеспечение

— документы, которые создают правовое пространство для функционирования ИБ;

# 3) модели безопасности

— схемы обеспечения ИБ, заложенные в данную конкретную информационную систему или среду;

# 4) криптография

— методы и средства преобразования информации в вид, затрудняющий или делающий невозможным несанкционированные операции с нею (чтение и/или модификацию), вместе с методами и средствами создания, хранения и распространения ключей — специальных информационных объектов, реализующих эти санкции;

# 5) антивирусное обеспечение

— средство для обнаружения и уничтожения зловредного кода (вирусов, троянских программ и т. п.);

# б) сканеры безопасности

— устройства проверки качества функционирования модели безопасности для данной конкретной информационной системы;

# 7) системы обнаружения атак

— устройства мониторинга активности в информационной среде, иногда с возможностью принятия самостоятельного участия в указанной активной деятельности;

# 8) резервное копирование

— сохранение избыточных копий информационных ресурсов на случай их возможной утраты или повреждения;

# 9) дублирование (резервирование)

— создание альтернативных устройств, необходимых для функционирования информационной среды, предназначенных для случаев выхода из строя основных устройств;

# 10) аварийный план

— набор мероприятий, предназначенных для претворения в жизнь, в случае если события происходят или произошли не так, как было предопределено правилами информационной безопасности;

# 11) обучение пользователей

— подготовка активных участников информационной среды для работы в условиях соответствия требованиям ИБ.

# Основные направления ИБ

# 1) Физическая безопасность

— обеспечение сохранности оборудования, предназначенного для функционирования информационной среды, контроль доступа людей к этому оборудованию;

защита самих пользователей информа- ционной среды от физического воздей- ствия злоумышленников;

защита информации не виртуального характера

## 2) Компьютерная безопасность (сетевая, телекоммуникационная, безопасность данных)

— обеспечение защиты информации в ее виртуальном виде.

# Место ИБ в национальной безопасности страны

Национальная безопасность России существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет только возрастать. **Почему? (В России, как и во всем мире, государственная тайна остается важнейшим инструментом защиты оборонных, экономических, политических и других важнейших интересов страны.)**

**Обеспечением ИБ в нашей стране занимаются органы федеральной службы безопасности по защите сведений, составляющих государственную тайну.**

Согласно «Стратегии национальной безопасности Российской Федерации до 2020 года», национальная безопасность — состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие России, оборону и безопасность государства.

Федеральной службой по техническому и экспортному контролю разработаны, а приказом Минздравсоцразвития России от 22 апреля 2009 г. № 205 утверждены «Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации», в соответствии с которыми современный специалист по защите информации должен уметь определять состав защищаемой информации, степень уязвимости, рассчитывать ущерб от возможной утраты информации, оценивать эффективность различных методов и средств защиты, проводить специальные исследования и сертификацию различных технических средств обработки и защиты информации, уметь проектировать и внедрять системы защиты информации, знать и использовать зарубежный опыт.

**Укрепление информационной безопасности названо в Концепции национальной безопасности РФ в числе самых важных долгосрочных задач**