

# ОРГАНИЗАЦИОННО- ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

# ВОПРОСЫ

- 1) Доктрина  
информационной  
безопасности РФ
- 2) Государственная  
тайна
- 3) Коммерческая тайна

# ФАКТОРЫ ВАЖНОСТИ ПРОБЛЕМЫ ИБ

- 1) повышением уровня доверия к автоматизированным системам управления и обработки информации, использованием их в критических технологиях;
- 2) обострением противоречий между объективно существующими потребностями общества в расширении свободного обмена информацией и чрезмерными или наоборот недостаточными ограничениями на ее распространение и использование;
- 3) многообразием видов угроз и возможных каналов несанкционированного доступа к информации;
- 4) ростом числа квалифицированных пользователей вычислительной техники и возможностей по созданию ими программно-математических воздействий на систему;
- 5) отсутствием достаточного количества квалифицированных специалистов в области защиты информации;

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.

## Объекты защиты:

- 1) информация и информационные ресурсы
- 2) носители информации
- 3) процессы обработки информации

# НОРМАТИВНО-ПРАВОВЫЕ АКТЫ В ОБЛАСТИ ИБ

## 1) Акты федерального законодательства:

- Международные договоры РФ;
- Конституция РФ;
- Законы федерального уровня (включая федеральные конституционные законы, кодексы);
- Указы Президента РФ;
- Постановления правительства РФ;
- Нормативные правовые акты федеральных министерств и ведомств;
- Нормативные правовые акты субъектов РФ, органов местного самоуправления и др.

## 2) К нормативно-методическим документам можно отнести

### а) Методические документы государственных органов России:

- Доктрина информационной безопасности РФ;
- Руководящие документы ФСТЭК (Гостехкомиссии России);
- Приказы ФСБ;

### б) Стандарты информационной безопасности, из которых выделяют:

- Международные стандарты;
- Государственные (национальные) стандарты РФ;
- Рекомендации по стандартизации;
- Методические указания.

# ОРГАНЫ\ПОДРАЗДЕЛЕНИЯ, ОБЕСПЕЧИВАЮЩИЕ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

1) Государственные органы РФ, контролирующие деятельность в области защиты информации:

- Комитет Государственной думы по безопасности;
- Совет безопасности России;
- Федеральная служба по техническому и экспортному контролю (ФСТЭК);
- Федеральная служба безопасности Российской Федерации (ФСБ России);
- Министерство внутренних дел Российской Федерации (МВД России);
- Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

2) Службы, организующие защиту информации на уровне предприятия

- Служба экономической безопасности;
- Служба безопасности персонала (Режимный отдел);
- Отдел кадров;
- Служба информационной безопасности.

# ОСНОВНЫЕ ИНФОРМАЦИОННЫЕ УГРОЗЫ И СОСТОЯНИЕ ИБ

10. Возможности трансграничного оборота информации все чаще используются для достижения геополитических, противоречащих международному праву военнополитических, а также террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности.

11. Одним из основных негативных факторов, влияющих на состояние информационной безопасности, является наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях.

13. Различные террористические и экстремистские организации широко используют механизмы информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников.

14. Возрастают масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий. При этом методы, способы и средства совершения таких преступлений становятся все изощреннее.

# ОСНОВНЫЕ ИНФОРМАЦИОННЫЕ УГРОЗЫ И СОСТОЯНИЕ ИБ

16. Состояние информационной безопасности в области государственной и общественной безопасности характеризуется постоянным повышением сложности, увеличением масштабов и ростом скоординированности компьютерных атак на объекты критической информационной инфраструктуры.

17. Состояние информационной безопасности в экономической сфере характеризуется недостаточным уровнем развития конкурентоспособных информационных технологий и их использования для производства продукции и оказания услуг. Остается высоким уровень зависимости отечественной промышленности от зарубежных информационных технологий.

18. Состояние информационной безопасности в области науки, технологий и образования характеризуется недостаточной эффективностью научных исследований, направленных на создание перспективных информационных технологий, низким уровнем внедрения отечественных разработок и недостаточным кадровым обеспечением в области информационной безопасности.

19. Существующее в настоящее время распределение между странами ресурсов, необходимых для обеспечения безопасного и устойчивого функционирования сети «Интернет», не позволяет реализовать совместное справедливое, основанное на принципах доверия управление ими.



# ОРГАНИЗАЦИОННЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

34. Деятельность государственных органов по обеспечению информационной безопасности основывается нескольких принципах.

35. Задачи государственных органов в рамках деятельности по обеспечению информационной безопасности.

36. Задачи государственных органов в рамках деятельности по развитию и совершенствованию системы обеспечения информационной безопасности.

37. Реализация настоящей Доктрины осуществляется на основе отраслевых документов стратегического планирования Российской Федерации.

38. Результаты мониторинга реализации настоящей Доктрины отражаются в ежегодном докладе Секретаря Совета Безопасности Российской Федерации Президенту Российской Федерации о состоянии национальной безопасности и мерах по ее укреплению.

# СОСТАВЛЯЮЩИЕ ГОСТАЙНЫ

## 1. Сведения в военной области:

- о содержании стратегических и оперативных планов и о других документах боевого управления; о подготовке и проведении военных операций, стратегическом и мобилизационном развертывании войск и об их важнейших показателях, характеризующих организацию, численность, дислокацию, боевую и мобилизационную готовность, боевую и другую военную подготовку, вооружение и материально-техническое обеспечение Вооруженных Сил, Пограничных войск и прочих воинских формирований;
- о направлении развития отдельных видов вооружения и военной техники, их количестве, тактико-технических характеристиках, организации и технологии производства, научно-исследовательских и опытно-конструкторских работах, связанных с разработкой новых образцов вооружения и военной техники, модернизации существующих образцов, а также о других работах, планируемых или осуществляемых в интересах страны;
- о силах и средствах Гражданской обороны, о готовности населенных пунктов, регионов и отдельных объектов к защите, эвакуации и рассредоточению населения, к обеспечению его жизнедеятельности и производственной деятельности объектов народного хозяйства в военное время или в условиях других чрезвычайных ситуаций;
- о геодезических, гравиметрических, картографических, гидрографических и гидрометеорологических данных и характеристиках, имеющих значение для обороны страны.

# СОСТАВЛЯЮЩИЕ ГОСТАЙНЫ

## 2. Сведения в области экономики, науки и техники:

- о мобилизационных планах и мощностях народного хозяйства, запасах и объемах поставок стратегических видов сырья и материалов, а также о размещении и объемах государственных мобилизационных материальных резервов;
- об использовании транспорта, связи, других отраслей и объектов инфра- структуры страны в интересах обеспечения ее безопасности;
- о содержании, объеме, финансировании и выполнении государственного оборонного заказа;
- о планах, объемах и других важнейших характеристиках добычи, производства и реализации отдельных стратегических видов сырья и продукции;
- о государственных запасах драгоценных металлов монетарной группы, драгоценных камней, валюты и других ценностей, об операциях, связанных с изготовлением денежных знаков и ценных бумаг, их хранением, охраной и защитой от подделки, обращением, обменом или изъятием, а также о других особых мерах финансовой деятельности государства.

# СОСТАВЛЯЮЩИЕ ГОСТАЙНЫ

## 3. Сведения в сфере внешних отношений:

- о директивах, планах, указаниях делегациям и должностным лицам по вопросам внешнеполитической и внешнеэкономической деятельности;
- о финансовой политике в отношении иностранных государств, а также о финансовой или денежно-кредитной деятельности, преждевременное распространение которых может нанести ущерб безопасности государства;
- о военном, научно-техническом и ином сотрудничестве с разными странами, если разглашение сведений об этом может нанести ущерб интересам государства;
- об экспорте и импорте вооружения, военной техники, отдельных стратегических видов сырья и продукции.

# СОСТАВЛЯЮЩИЕ ГОСТАЙНЫ

4. сведения в области государственной безопасности и охраны правопорядка:

- о силах, средствах, источниках, планах и результатах разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также данные о финансировании этой деятельности, если они раскрывают перечисленные сведения;
- о лицах, которые сотрудничают или раньше сотрудничали на конфиденциальной основе с органами. Осуществляющими такую деятельность;
- об организации, о силах, средствах и методах обеспечения безопасности объектов государственной охраны, а также данные о финансировании этой деятельности, если они раскрывают перечисленные сведения;
- о системе президентской, правительственной, шифрованной, в том числе кодированной и засекреченной связи, о шифрах, о разработке, об изготовлении шифров и обеспечении ими, о методах и средствах анализа шифровальных средств и средств специальной защиты, об информационно-аналитических системах специального назначения;
- о методах и средствах защиты секретной информации;
- об организации и о фактическом состоянии защиты государственной тайны;
- о защите Государственной границы Российской Федерации;
- о расходах федерального бюджета, связанных с обеспечением обороны, безопасности государства и правительственной деятельности в РФ;
- о разработке и использовании шифров, работе с ними, проведении научно-исследовательских работ в области криптографии;
- о подготовке кадров, раскрывающие мероприятия, проводимые в целях обеспечения безопасности государства.

# УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА СПОСЯГАТЕЛЬСТВО НА ГОСТАЙНУ

- шпионаж (ст. ст. 275, 276 УК РФ);
- выдача государственной тайны иностранному государству, иностранной организации или их представителям ( ст. 275 УК РФ);
- иное оказание помощи иностранному государству, иностранной организации или их представителям ( ст. 275 УК РФ);
- разглашение государственной тайны (ст. 283 УК РФ);
- утрата документов, содержащих гостайну, или предметов, сведения о которых составляют гостайну (ст. 284 УК РФ);
- уничтожение, блокирование, модификация или копирование охраняемой законом компьютерной информации ( в том числе содержащей государственную тайну) в результате неправомерного доступа к ней (ст. 272 УК РФ) или нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК РФ);
- поставление охраняемой законом компьютерной информации (в том числе содержащей государственную тайну) в заведомую опасность несанкционированного уничтожения, блокирования или копирования в результате создания или распространения вредоносных программ для ЭВМ (ст. 283 УК РФ);
- похищение, уничтожение, повреждение или сокрытие официальных документов ( в том числе содержащих государственную тайну) (ст. 325, часть 1 УК РФ).

# КОММЕРЧЕСКАЯ ТАЙНА

**Коммерческая тайна** - конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

**Информация, составляющая коммерческую тайну**, - научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства «ноу-хау»), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам. К такой информации нет свободного доступа на законном основании и в отношении нее обладателем информации введен режим коммерческой тайны.

# СВЕДЕНИЯ, КОТОРЫЕ НЕ МОГУТ СОСТАВЛЯТЬ КОММЕРЧЕСКУЮ ТАЙНУ

- 1) содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;
- 2) содержащихся в документах, дающих право на осуществление предпринимательской деятельности;
- 3) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;
- 4) о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;
- 5) о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;
- 6) о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;
- 7) о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;
- 8) об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;
- 9) о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;
- 10) о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;
- 11) обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.



## Статья 13.14 Кодекса об административных правонарушениях

Разглашение информации, доступ к которой ограничен ФЗ (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, влечет наложение административного штрафа.

## Статья 183 УК РФ «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну»

1. Собираение сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом наказывается штрафом в размере до 80 тысяч рублей или в размере заработной платы или иного дохода осужденного за период от 1 до 6 месяцев либо лишением свободы на срок до 2-х лет.

2. Незаконные разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе, наказывается штрафом в размере до 120 тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет либо лишением свободы на срок до 3 лет.

3. Те же деяния, причинившие крупный ущерб или совершенные из корыстной заинтересованности, наказывается штрафом в размере до 200 тысяч рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет либо лишением свободы на срок до 5 лет.

4. Деяния, предусмотренные частями 2-й или 3-ей статьи 183, повлекшие тяжкие последствия, наказывается лишением свободы на срок до 10 лет.