РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА
И ГОСУДАРСТВЕННОЙ СЛУЖБЫ
ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Панкратов И.Ю., научный сотрудник НИЦГУ, доцент кафедры информатики и прикладной математики, канд. экон. наук

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРОГРАММА КУРСА

- 1. Основные понятия информационной безопасности и защиты информации
- 2. Угрозы информационной безопасности
- 3. Политика информационной безопасности
- 4. Стандарты информационной безопасности
- 5. Принципы многоуровневой защиты корпоративной информации
- 6. Безопасность операционных систем
- 7. Криптографическая защита
- информации
- 8. Защита от вредоносных программ и спама

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЛИТЕРАТУРА

Актуальность

Во-первых

распределенные корпоративные информационные системы становятся сегодня важнейшим средством производства современной компании, они позволяют преобразовать традиционные формы бизнеса в электронный бизнес, важнейшим условием существования которого является информационная безопасность

Во-вторых

широкое распространение Интернета и появление новых информационных технологий, в частности, облачных сервисов, социальных сетей, мобильного интернета, а также необходимость обработки больших данных обусловливает необходимость разработки современных средств защиты информации

В-третьих

ключевое значение на рынке банковских услуг приобретают электронные платежные системы, технологии дистанционного банковского обслуживания - электронного банкинга, мобильного банка и другие, предъявляющие новые требования к информационной безопасности

В-четвертых

Наступило время , не просто киберпреступников и интернет-мошенников, а кибертерроризма, кибероружия и кибервойн».

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ОСНОВНЫЕ ДРАЙВЕРЫ РАЗВИТИЯ ФИНАНСОВО-ЭКОНОМИЧЕСКИХ ОТНОШЕНИЙ

- Модернизация инфраструктуры
- Автоматизация дорогостоящих процедур
- Сокращение участия посредников
- Стратегическая опора на данные
- Специализация продуктов
- Расширение возможностей пользователей

Увеличение числа субъектов сети, усложнение структуры их взаимодействия, наличие неопределенностей в правовой среде – все это меняет характер рисков, расширяя требования по защите информации и дополняя их задачами по формированию нового сетевого поведения.

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

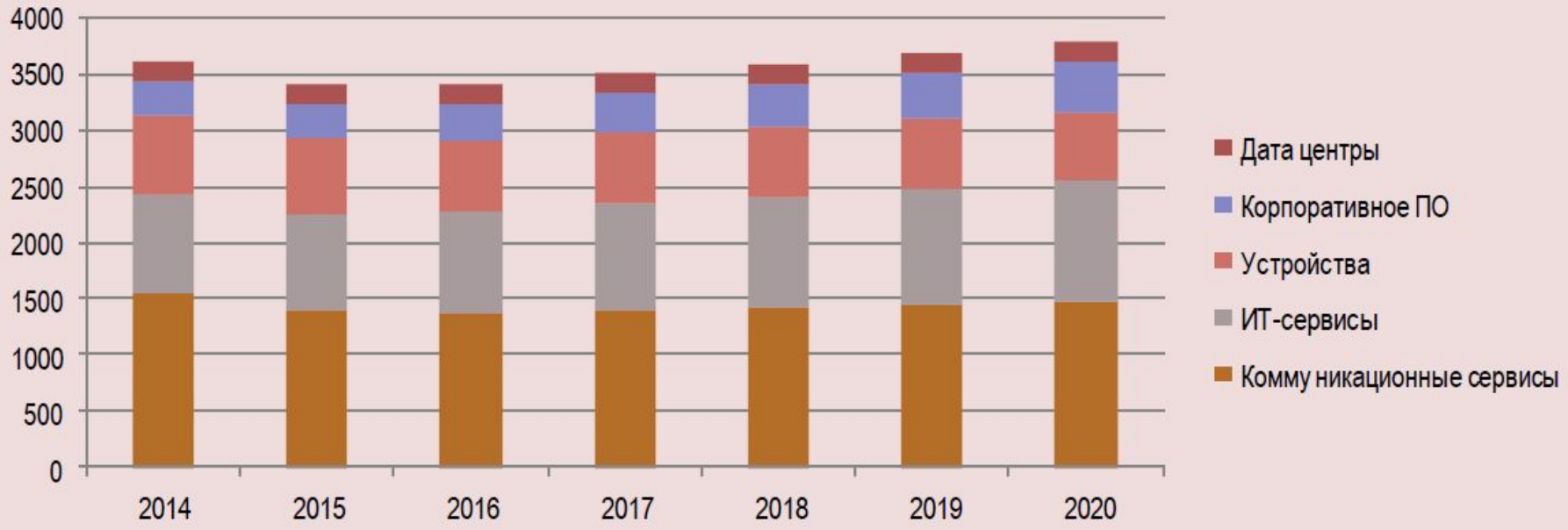
$3,54 трлн — объем затрат на ИТ в мире

429 млн — записей, относящихся к персональным данным, были украдены или потеряны в мире в 2015 году

$75 млрд — затрачено на кибербезопасность в 2015 году

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЕЖЕГОДНЫЕ СОВОКУПНЫЕ ЗАТРАТЫ НА ИТ В МИРЕ (АКТУАЛЬНЫЕ ДАННЫЕ И ПРОГНОЗ), $ МЛРД



Источники: Forecast Alert. IT Spending, Worldwide, 2Q16 Update, Gartner.

Уровень потерь от киберпреступности в крупнейших экономиках

Страна	Объем ВВП, $ трлн**	Потери, % от ВВП***	Потери, $ млрд****
США	16,8	0,64	108
Китай	9,5	0,63	60
Япония	4,9	0,02	0,98
Германия	3,7	1,60	59
Франция	2,8	0,11	3

Страна	Объем ВВП, $ трлн**	Потери, % от ВВП***	Потери, $ млрд****
Великобритания	2,7	0,16	4,3
Бразилия	2,4	0,32	7,7
Россия	2,1	0,10	2
Италия	2,1	0,04	0,9
Индия	1,9	0,21	4

*По итогам 2013 года

**Данные World Bank

***Estimating the Global Cost of Cyber-Crime, CSIS/McAfee

****Данные Allianz Global Corporate & Specialty

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА
И ГОСУДАРСТВЕННОЙ СЛУЖБЫ
ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЛЕКЦИЯ 1. ОСНОВНЫЕ ПОНЯТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

Информационная безопасность

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. ЧТО ЭТО?

ГОСТ Р50922–2006

защищенность информации от незаконного ознакомления, преобразования и уничтожения, а также защищенность информационных ресурсов от воздействий, направленных на нарушение их)

Стандарт Банка России

Состояние защищенности интересов (целей) организации БС РФ в условиях угроз в информационной сфере

ISO/IEC 27000:2009

Preservation of confidentiality, integrity and availability of information.

Доктрина информационной безопасности РФ 2016

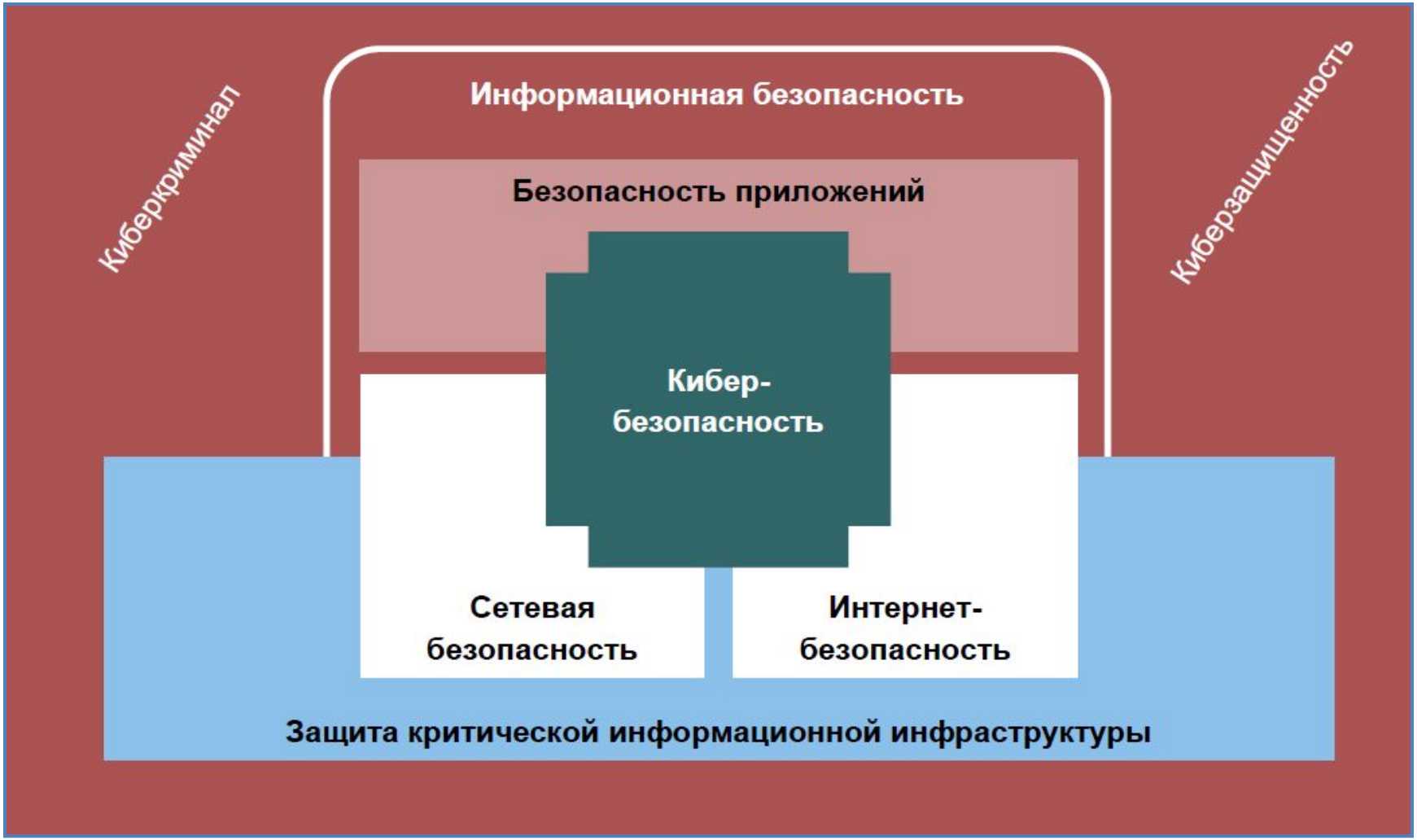
состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие РФ оборона и безопасность

Committee on National Security Systems (CNSS)

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ВЗАИМОСВЯЗЬ КИБЕРБЕЗОПАСНОСТИ И СМЕЖНЫХ ПОНЯТИЙ



НАЦИОНАЛЬНЫЕ ИНТЕРЕСЫ В ИНФОРМАЦИОННОЙ СФЕРЕ

Доктрина Информационной безопасности РФ 2016

национальные интересы Российской Федерации в информационной сфере - объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития в части, касающейся информационной сферы;

-обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации;

- доведение до российской и международной общественности достоверной информации о государственной политике Российской Федерации и ее официальной позиции по социально значимым событиям в стране и мире, применение информационных технологий в целях обеспечения национальной безопасности Российской Федерации в области культуры;

- содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности, на укрепление равноправного стратегического партнерства в области информационной безопасности, а также на защиту суверенитета Российской Федерации в информационном пространстве.

НАЦИОНАЛЬНЫЕ ИНТЕРЕСЫ В БС РФ

создание условий для совершенствования элементов национальной банковской системы, способной к эффективному регулированию банковских рисков, капитала и ликвидности, а также государственных финансовых потоков в объемах, необходимых для выполнения государственных задач и функций с целью достижения экономического суверенитета Российской Федерации

создание условий для формирования устойчивой банковской системы, предоставляющей доступ хозяйствующих субъектов к долгосрочным кредитам с обоснованной процентной ставкой на финансирование капитальных вложений, инноваций и импортозамещающих производств.

создание и безопасное использование современных передовых банковских продуктов и услуг, в том числе, интернет-банкинг, мобильный банк и т.д.

создание условий для предотвращения бесконтрольного вывоза капитала; для обеспечения стабильности рубля как национальной валюты;

CIA (КЦД) концепт (Конфиденциальность)

Шангин В.

Это статус, предоставленный данным и определяющий требуемую степень их защиты. Конфиденциальная информация должна быть известна только допущенным и прошедшим проверку (авторизованным) субъектам системы (пользователям, процессам, программам). Для остальных субъектов системы эта информация должна быть неизвестной.

Except ISO27000

In information security, confidentiality «is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes»

Стандарт Банка России

Свойство ИБ организации БС РФ, состоящее в том, что обработка, хранение и передача информационных активов осуществляется таким образом, что информационные активы доступны только авторизованным пользователям, объектам системы или процессам

Стандартное определение

состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право

CIA (КЦД) концепт (Доступность)

Шангин В.

возможность за приемлемое время получить требуемую информационную услугу.

Стандарт Банка России

Свойство ИБ организации БС РФ, состоящее в том, что информационные активы предоставляются авторизованному пользователю, причем в виде и месте, необходимых пользователю, и в то время, когда они ему необходимы.

Except ISO27000

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly.

Стандартное определение

свойство информационных ресурсов, в том числе информации, определяющее возможность их получения и использования по требованию уполномоченных лиц

CIA (КЦД) концепт (Целостность)

Шангин В.

подразумеваются актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Except ISO27000

In information security, data integrity means maintaining and assuring the accuracy and completeness of data over its entire life-cycle. This means that data cannot be modified in an unauthorized or undetected manner.

Стандарт Банка России

Свойство ИБ организации БС РФ сохранять неизменность или исправлять обнаруженные изменения в своих информационных активах.

Стандартное определение

неизменность информации в процессе ее передачи или хранения, избежание несанкционированной модификации информации;

КИБЕРБЕЗОПАСНОСТЬ КАК КУЛЬТУРА (РЕЗОЛЮЦИЯ ООН «СОЗДАНИЕ ГЛОБАЛЬНОЙ КУЛЬТУРЫ КИБЕРБЕЗОПАСНОСТИ»)

- **Осведомленность;**
- **Ответственность;**
- **Реагирование;**
- **Этика -** учитывать законные интересы других и признавать, что их действия или бездействие могут повредить другим;
- **Демократия;**
- **Оценка риска;**
- **Проектирование и внедрение средств обеспечения безопасности -** рассматривать безопасность в качестве важнейшего элемента планирования и проектирования, эксплуатации и использования информационных систем и сетей;
- **Управление обеспечением безопасности** - Участники должны принять комплексный подход к управлению обеспечением безопасности, опираясь на динамичную оценку риска, охватывающую все уровни деятельности участников и все аспекты их операций;
- **Переоценка**

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЭКОНОМИЧЕСКИЙ ПОДХОД К КИБЕРБЕЗОПАСНОСТИ

- Кибербезопасность – вопрос управления рисками всего предприятия, а не составляющая часть его ИТ-платформы.
- Высший менеджмент должен понимать связь киберрисков и регуляторных требований. Стандартов много, они различны в разных юрисдикциях, ситуация в правовом поле стремительно меняется, поэтому важно понимать нормативную сторону вопроса максимально полно.
- Советы директоров (СД) должны иметь доступ к экспертизе в части кибербезопасности. Этот вопрос может быть решен либо включением в СД профильного профессионала, либо как минимум уделению кибербезопасности достаточного внимания на заседаниях СД.
- Директорам необходимо установить требования по наличию у организаций рабочих органов, связанных с обеспечением кибербезопасности и действующих в масштабах всего предприятия.
- Руководство организаций должно располагать методами оценки ущерба, возникшего вследствие событий в киберсреде и планами по его нивелированию, то есть должны применяться современные механизмы управления финансовыми рисками.

ОСНОВНЫЕ ПОНЯТИЯ ЗАЩИТЫ ИНФОРМАЦИИ

Защита информации - деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемый объект.

Система информационной безопасности; СИБ - совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение

под **объектами системы** понимают пассивные компоненты системы, хранящие, принимающие или передающие информацию.

под **субъектами системы** понимают активные компоненты системы, которые могут стать причиной потока информации от объекта к субъекту или изменения состояния системы. В качестве субъектов могут выступать пользователи, активные программы и процессы

В последнее время все больше используют такие термины как киберпространство, кибербезопасность, киберугроза, уязвимость киберпространства, киберпреступность и другие.

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОНЯТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ИХ ВЗАИМОСВЯЗЬ

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Угроза информационной безопасности

Шангин В.

совокупность условий или действий, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Стандарт Банка России

Угроза нарушения свойств ИБ - доступности, целостности или конфиденциальности информационных активов организации БС РФ.

Уязвимость – свойство информационной системы, обусловливающее возможность реализации угрозы безопасности обрабатываемой в ней информации.

Доктрина ИБ 2016

угроза информационной безопасности Российской Федерации - совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере;

National Information Assurance Glossary

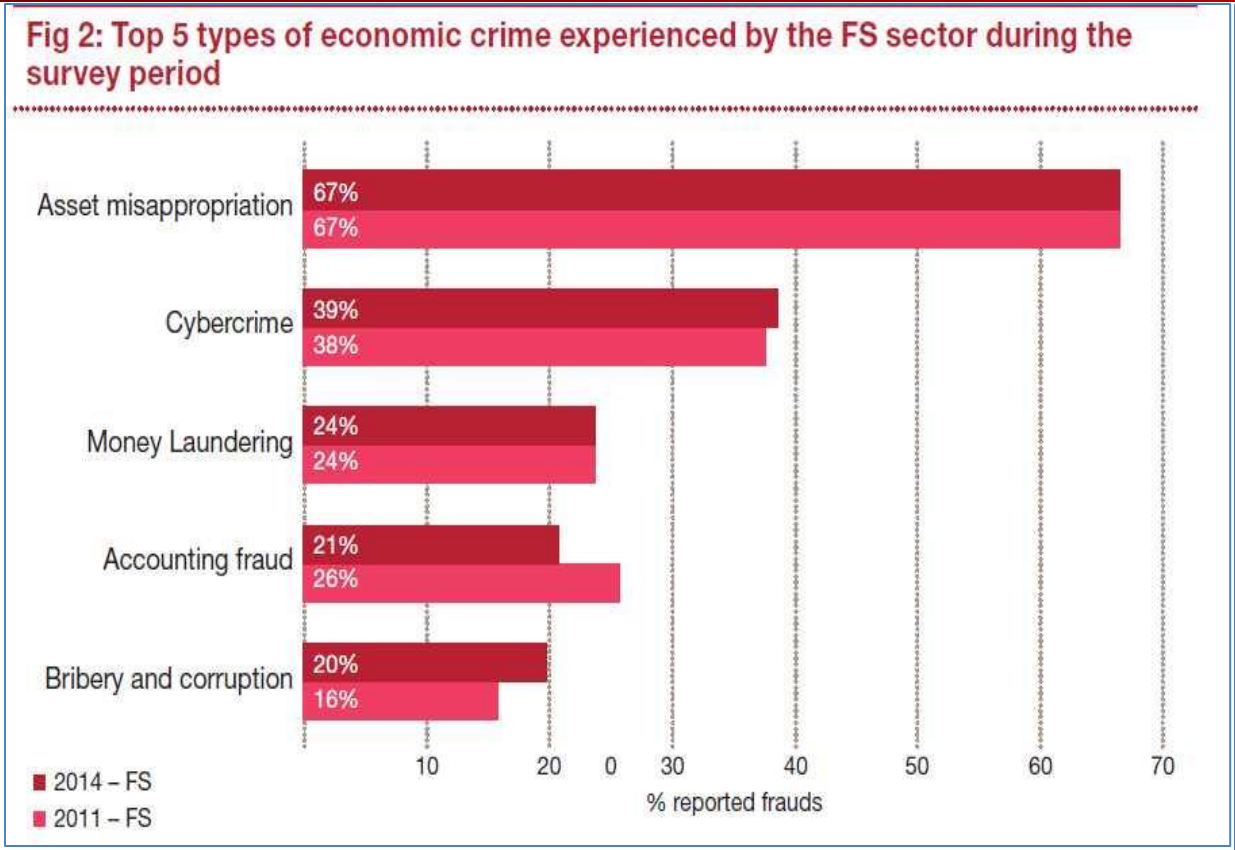
Any circumstance or event with the potential to adversely impact an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Угрозы информационной безопасности по Доктрине ИБ 2016

- наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях.
- деятельность организаций, осуществляющих техническую разведку в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса.
- использование специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств.
- увеличение в зарубежных средствах массовой информации объема материалов, содержащих предвзятую оценку государственной политики Российской Федерации.
- информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей.
- постоянное повышение сложности, увеличение масштабов и рост скоординированности компьютерных атак на объекты критической информационной инфраструктуры, усилением разведывательной деятельности иностранных государств в отношении Российской Федерации.
- высокий уровень зависимости отечественной промышленности от зарубежных информационных технологий в части, касающейся электронной компонентной базы, программного обеспечения, вычислительной техники и средств связи, что обусловливает зависимость социально-экономического развития Российской Федерации от геополитических интересов зарубежных стран.

УГРОЗЫ В ФИНАНСОВОМ СЕКТОРЕ, PWC



«Киберпреступление» - «... Экономическое преступление, совершенное с использованием компьютера и интернета ... и включает в себя только такие экономические преступления, где компьютер, интернет, использование электронных носителей и устройств является основным , а не случайным элементом» (например, «распространение вирусов, незаконная загрузка медиа, фишинг и фарминг и кража личной информации, такой как банковские реквизиты»

Киберпреступность - преступная деятельность, в которой техническая инфраструктура киберпространства используется в целях преступления или является целью преступления, или где киберпространство является источником, инструментом, целью или местом преступления.

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Оценка направлений воздействия киберпреступлений представителями бизнеса

Источники: Global Economic Crime Survey 2016, PwC.

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЗАВИСИМОСТЬ ВОСПРИЯТИЯ КИБЕРПРЕСТУПЛЕНИЙ ОТ ФУНКЦИОНАЛА

«Today's incidents, yesterday's strategies – As the digital channel in financial services continues to evolve, cybersecurity has become a business risk, rather than simply a technical risk» (The Global State of Information Security® Survey, PwC, CIO magazine, and CSO magazine)

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ВЫБОР ПРЕДСТАВИТЕЛЯМИ БИЗНЕСА СЕКТОРОВ, НАИБОЛЕЕ ПРИВЛЕКАТЕЛЬНЫХ ДЛЯ КИБЕРПРЕСТУПНИКОВ

Источники: *Cybercrime survey report 2015, KPMG in India.*

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ДОМАШНЕЕ ЗАДАНИЕ

Задание: Просмотрите Интернет-ресурсы (например, banki.ru) на факты кибермошенничества в отношении клиентов этих банков, выберите один случай и постарайтесь ответить на следующие вопросы:

- Сформулируйте интересы клиента банка, которые были затронуты в данном случае;
- Перечислите угрозы интересам клиента банка, характерные для данного случая;
- Назовите основные объекты и субъекты системы обеспечения информационной безопасности, затронутые в данном случае?
- Перечислите возможные каналы и способы доступа к банковскому счету клиента с целью хищения денежных средств, используемые злоумышленниками в данном случае

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Рейтинг интернет-банков для частных лиц

№	Интернет-банк	Оценка*
1	Промсвязьбанк	**79,8** (8,2 / 4,1)
2	Тинькофф Банк	**79,5** (7,9 / 4,2)
3	Альфа-Банк	**78,3** (7,9 / 4,1)
4	Запсибкомбанк	**72,5** (7,5 / 3,8)
5	МДМ Банк	**69,7** (6,4 / 4)
6	Банк Санкт-Петербург	**68,5** (7,4 / 3,5)
7	Банк Москвы	**67,5** (6,5 / 3,8)
8	Московский Кредитный Банк	**64,3** (6,6 / 3,5)
9	Банк Траст	**63,9** (6 / 3,7)
10	Банк Русский Стандарт	**63,8** (6,5 / 3,5)

№	Интернет-банк	Оценка*
11	УБРиР	**63,6** (6,7 / 3,4)
12	Сбербанк России	**62,5** (6 / 3,6)
13	Банк Уралсиб	**61,1** (5,4 / 3,7)
14	АК БАРС	**57,1** (5,4 / 3,4)
15	ВТБ24	**56,8** (5,6 / 3,3)
16	Банк Открытие	**56,1** (5,2 / 3,4)
17	СМП Банк	**55,8** (5,4 / 3,3)
18	Восточный Банк	**55,3** (4,7 / 3,5)
19	Хоум Кредит Банк	**54,3** (5,1 / 3,3)
20	Банк Авангард	**54,2** (6,2 / 2,8)

№	Интернет-банк	Оценка*
21	МТС Банк	**53,5** (5,2 / 3,2)
22	Бинбанк	**53,1** (5,6 / 3)
23	ОТП Банк	**51,4** (3,7 / 3,5)
24	Банк Казани	**51** (5,2 / 3)
25	ЮниКредит Банк	**50,8** (5,6 / 2,8)
26	Райффайзенбанк	**50** (5 / 3)
27	Русский Трастовый Банк	**49,8** (4,4 / 3,2)
28	Ситибанк	**49,5** (4,9 / 3)
29-30	Банк Возрождение	**48** (3,6 / 3,3)
	Росбанк	**48** (4,3 / 3,1)
	ЦТБ**	**47,3** (4,7 / 2,9)
31	Россельхозбанк	**46,6** (4,3 / 3)
32	ИнтерПрогрессБанк	**41,6** (3,8 / 2,8)
33	Ренессанс Кредит	**41,4** (2 / 3,2)
34	Газпромбанк	**39,5** (3,9 / 2,6)
35	Кредит Европа Банк	**36,8** (3,6 / 2,5)

* Итоговая оценка эффективности интернет-банка по шкале от 0 до 100 баллов. В скобках приведены оценки функциональных возможностей интернет-банка по шкале от 0 до 10 баллов и оценка удобства пользования по шкале от 1 до 5 баллов.

** Программное решение компании ЦТБ (Цифровые Технологии Будущего) обследовалось на тестовом сервере без подключения к работающим сервисам банка. Оценка приводится без места в рейтинге в качестве иллюстрации возможного уровня эффективности реального интернет-банка, построенного на данном решении.

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА
И ГОСУДАРСТВЕННОЙ СЛУЖБЫ
ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

СПАСИБО ЗА ВНИМАНИЕ!

Информационная безопасность