ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКОВ РЕСПУБЛИКИ БЕЛАРУСЬ

Вячеслав Аксёнов

13-17.03.2023

ПРОГРАММА КУРСА

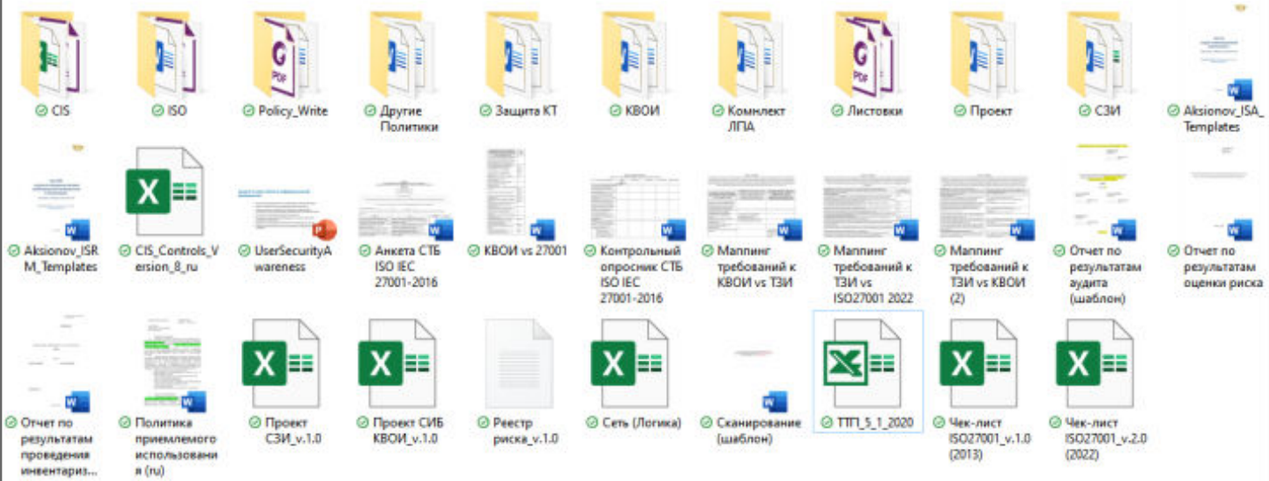
1. Структуры и стандарты построения систем ИБ на основании процессного подхода
2. Защита информации в информационных системах Банка
3. Обеспечения кибербезопасности на критически важных объектах информационной инфраструктуры Банка
4. Разработка (совершенствование) системы менеджмента информационной безопасности в Банке
5. Управления программой аудита информационной безопасности Банка
6. Менеджмент риска информационной безопасности (киберриска)

ТТП ИБ

ПРАКТИЧЕСКИЕ ЗАДАНИЯ

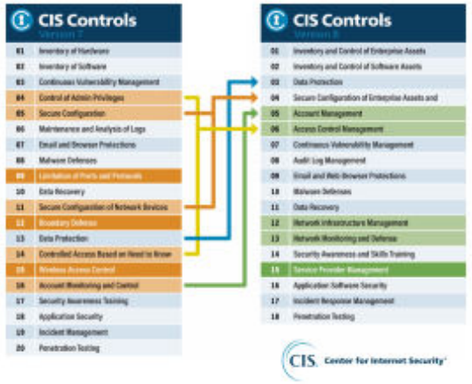
1. Проект разработки и внедрения системы защиты информации
2. Проект разработки и внедрения системы информационной безопасности критически важного объекта информатизации
3. Разработка и планирование внедрения процесса системы менеджмента информационной безопасности
4. Проведение аудита информационной безопасности
5. Оценка риска нарушения информационной безопасности

ДОПОЛНИТЕЛЬНЫЕ МАТЕРИАЛЫ



CIS Controls

https://www.cisecurity.org



CIS RAM

CIS CSAT

NIST

National Institute of Standards and Technology

NIST Special Publication 800-53 Revision 5

Security and Privacy Controls for Information Systems and Organizations

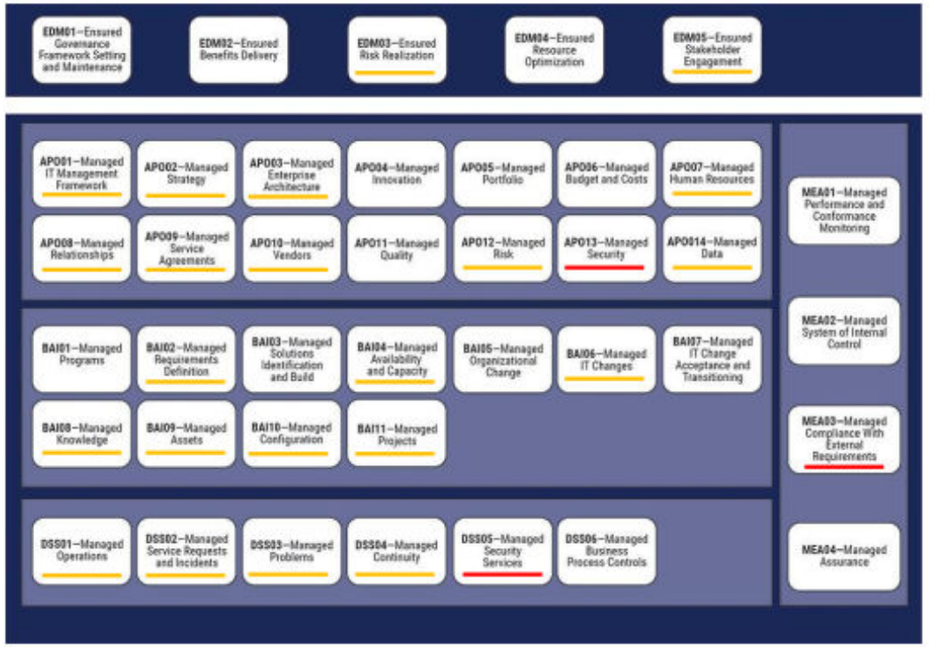
ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

COBIT

An ISACA Framework

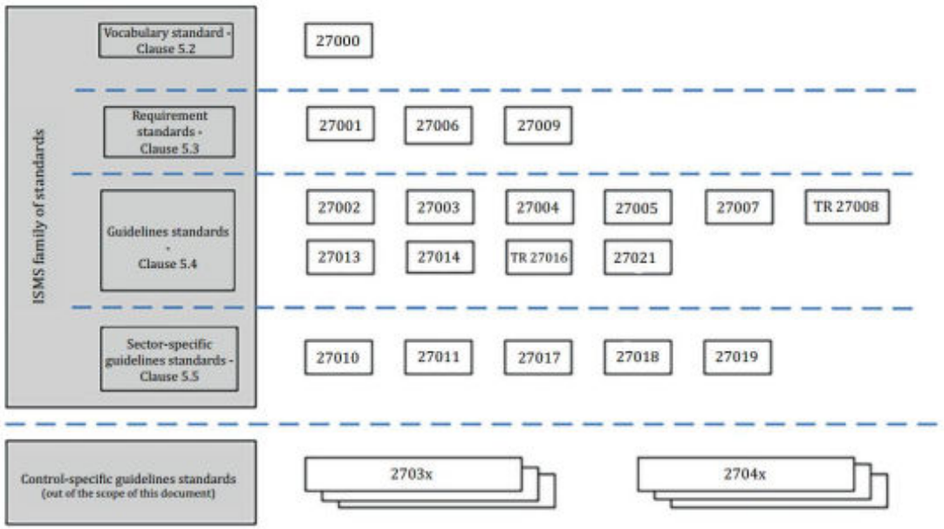
Governance and Management Objectives in COBIT 2019

- ✓ Evaluate, Direct and Monitor (EDM)
- ✓ Align, Plan and Organize (APO)
- ✓ Build, Acquire and Implement (BAI)
- ✓ Deliver, Service and Support (DSS)
- ✓ Monitor, Evaluate and Assess (MEA)



ISO

International Organization for Standardization



Закон РБ от 10.11.2008 г. № 455-З **«Об информации, информатизации и защите информации»**

Закон РБ от 05.01.2013 г. № 16-З **«О коммерческой тайне»**

Закон РБ от 07.05.2021 г. № 99-З **«О защите персональных данных»**

Положение о технической и криптографической защите информации
Указ Президента РБ от 16.04.2013 № 196 (в редакции Указа Президента РБ от 09.12.2019 № 449)

О служебной информации ограниченного распространения и информации, составляющей коммерческую тайну
Постановление Совета Министров РБ от 12 августа 2014 г. № 783

Технический регламент Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY)
Постановление Совета Министров РБ 15.05.2013 № 375 (в редакции постановления Совета Министров РБ 12.03.2020 № 145)

Перечень государственных стандартов, взаимосвязанных с техническим регламентом Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY)
Приказ ОАЦ от 12.03.2020 № 77

Положение о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено
Приказ ОАЦ от 20.02.2020 № 66 (в редакции приказа от 12.11.2021 № 195)

Положение о порядке технической и криптографической защиты информации, обрабатываемой на критически важных объектах информатизации
Приказ ОАЦ от 20.02.2020 № 66 (в редакции приказа от 12.11.2021 № 195)

Положение о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено
Приказ ОАЦ от 20.02.2020 № 66

Государственное регулирование

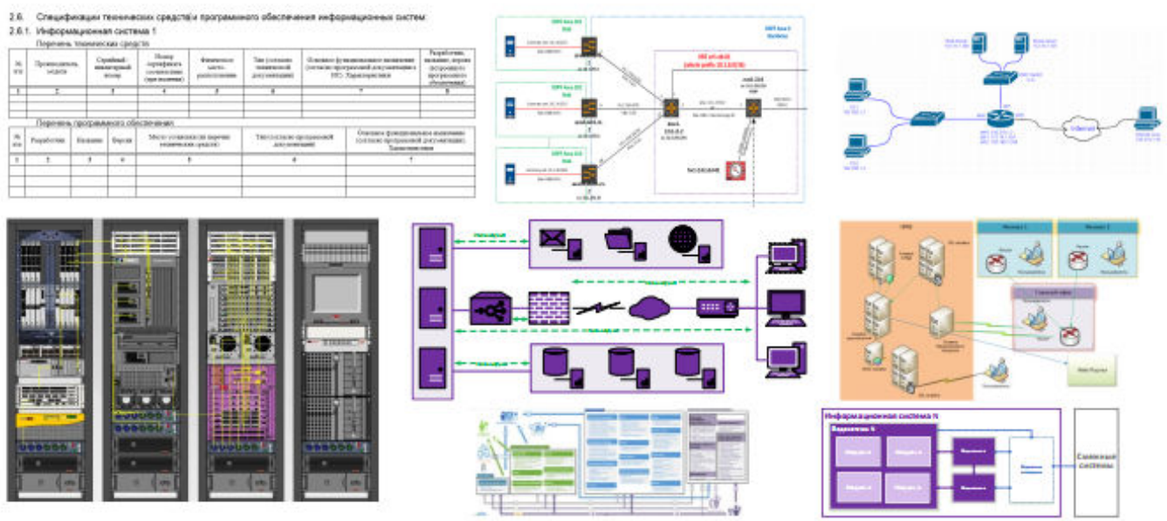
ПРЕЗИДЕНТ
Республики Беларусь

Оперативно-аналитический центр при Президенте Республики Беларусь

Национальный центр защиты персональных данных Республики Беларусь

Анализ структуры ИС

Проектирование СЗИ



Перечень требований к СЗИ

Приложение 3 к Приказу ОАЦ №66

Класс ИС	Rout	FW	Proxy / WAF	IDS	AV EP	AV NET	AV MAIL	VPN	Pre-crypt	IC	IDM	AM	DLP	LM
3-дсп	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕			⊕	⊕	⊕	⊕
3-юл	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕			⊕	⊕		
3-бг	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕		⊕
3-спец	⊕	⊕	⊕	⊕	⊕		⊕	⊕						⊕
3-ин	⊕	⊕	⊕	⊕	⊕		⊕	⊕						⊕
4-дсп					⊕									
4-юл					⊕									
4-бг					⊕				⊕	⊕				⊕
4-спец					⊕									
4-ин					⊕									

п.10. Собственник (владелец) ИС **вправе не включать** в техническое задание **отдельные обязательные требования** к СЗИ при отсутствии в ИС соответствующего объекта (технологии) либо при условии согласования с ОАЦ закрепления в таком техническом задании обоснованных компенсирующих мер

СИСТЕМА ИБ КВОИ

люди	Руководитель	Подразделение ИБ	Подразделение ИТ	Персонал	
процессы	Управление активами	Управление идентификацией и аутентификацией	Управление непрерывностью	Повышение осведомленности и обучение	
	Управление риском	Управление доступом	Управление инцидентами	Управление соответствием	Мониторинг	Внутренний контроль
технологии	Сетевая безопасность	Защита от несанкционированного доступа	Криптографическая защита	Регистрация и анализ событий	Резервное копирование
	Антивирусная защита		Контроль целостности	Юридически значимый аудит	Оценка защищенности

Проектирование системы ИБ КВОИ:

Этап	Результат
15.1. определение внутренних (организационная структура, информационные системы, информационные потоки и процессы) и внешних (взаимосвязи с контрагентами и другое) границ, оказывающих влияние на обеспечение ИБ КВОИ;	Отчет о проведении обследования КВОИ
15.2. определение целей обеспечения ИБ КВОИ, совместимых с процессами деятельности владельца КВОИ и прогнозными документами организации;	Отчет о проведении обследования КВОИ
15.3. инвентаризация (выявление и учет), а также определение степени важности для основной деятельности владельца КВОИ (исходя из конфиденциальности, целостности и доступности) активов КВОИ;	Реестр активов КВОИ
15.4. определение работников, ответственных за использование активов КВОИ;	Отчет о проведении обследования КВОИ Раздел в Политику ИБ
15.5. определение физических и логических границ области применения системы ИБ с использованием структурной и логической схем КВОИ;	Формуляр КВОИ Структурная схема Логическая схема
15.6. определение угроз ИБ КВОИ;	Реестр (каталог) угроз КВОИ
15.7. разработка методологии (методики) оценки рисков ИБ КВОИ и оценка таких рисков;	Методика оценки рисков Отчет по результатам оценки рисков
15.8. определение требований к параметрам настройки программных и программно-аппаратных средств, включая средства ЗИ, по обеспечению ИБ КВОИ, блокированию (нейтрализации) угроз ИБ КВОИ;	Положение по администрированию КВОИ
15.9. определение средств управления, необходимых для реализации выбранного варианта обработки рисков ИБ КВОИ.	План обработки рисков

Проектирование системы ИБ КВОИ
- Определение контекста
- Определение целей обеспечения ИБ
- Инвентаризация активов
- Определение организационной структуры системы ИБ КВОИ
- Определение области применения системы ИБ КВОИ
- Определение угроз ИБ КВОИ
- Разработка методики оценки рисков ИБ КВОИ
- Оценка рисков ИБ КВОИ
- Разработка плана обработки рисков ИБ КВОИ

Создание системы ИБ КВОИ
- Разработка политики ИБ КВОИ
- Реализация мер по ЗИ КВОИ:
  - идентификация и аутентификация
  - управление доступом к активам КВОИ
  - обращение с носителями информации
  - аудит ИБ
  - защита от вредоносного ПО
  - управление процедурами резервирования:
  - обеспечение ИБ КВОИ и его
- Разработка плана восстановления КВОИ
- конфигурацией
- обновление ПО

Аудит системы ИБ КВОИ
- Анализ и оценка соответствия системы ИБ требованиям
- Проведение контроля эффективности защищенности системы ИБ;
- Формирование замечаний (недостатков), выявленных в процессе аудита, и предложений по их
- Составление акта по форме согласно приложению и рекомендаций по результатам аудита.

Функционирование системы ИБ КВОИ
- Эксплуатация мер по ЗИ КВОИ
- Повышение уровня знаний по обеспечению ИБ КВОИ
- Контроль за состоянием активов КВОИ для выявления потенциальных
- Анализ и оценка угроз ИБ КВОИ
- Аудит системы ИБ КВОИ

14. Комплекс мероприятий по технической и криптографической ЗИ, обрабатываемой на КВОИ, включает проектирование, создание и аудит системы ИБ.

Меры по ЗИ КВОИ

20. В системе информационной безопасности в зависимости от угроз информационной безопасности критически важного объекта информатизации реализуются следующие организационные и технические меры:

- 20.1. идентификация и аутентификация
- 20.2. управление доступом к активам КВОИ
- 20.3. обращение с носителями информации
- 20.4. аудит ИБ
- 20.5. защита от вредоносного ПО
- 20.6. управление процедурами резервирования
- 20.7. обеспечение ИБ КВОИ и его элементов
- 20.8. управление конфигурацией
- 20.9. обновление ПО
- 20.10. планирование мероприятий по обеспечению ИБ КВОИ
- 20.11. реагирование на события ИБ КВОИ и управление ими
- 20.12. информирование и обучение персонала

Создание системы ИБ КВОИ

ISO/IEC 27001:2022

6. Планирование

6.1 Действия по рассмотрению рисков и возможностей

- 6.1.1 Общие требования
- 6.1.2 Оценка риска информационной безопасности
- 6.1.3 Обработка рисков информационной безопасности

6.2 Цели информационной безопасности и планирование их достижения

6.3 Planning of changes

When the organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner.

Statement of Applicability

Current as of: DD/MM/YYYY

Legend (for Selected Controls and Reasons for controls selection)

LR: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

ISO/IEC 27001:2013 Annex A controls			Current controls	Remarks (with justification for exclusions)	Selected controls and reasons for selection				Remarks (overview of implementation)
Clause	Sec	Control Objective/Control			LR	CO	BR/BP	RRA	
5 Security Policies	5.1	Management direction for information security							
	5.1.1	Policies for information							
	5.1.2	Review of the policies for information security							
6 Organisation of information security	6.1	Internal organisation							
	6.1.1	Information security roles and responsibilities							
	6.1.2	Segregation of duties							
	6.1.3	Contact with authorities							
	6.1.4	Contact with special interest groups							
	6.1.5	Information security in project management							
	6.2	Mobile devices and teleworking							

Section	Information security control	Control
A5	Organizational controls	
A.5.1	Политики информационной безопасности	Политика информационной безопасности и тематические политики должны быть определены, утверждены руководством, опубликованы, доведены до сведения и подтверждены соответствующим персоналом и соответствующими заинтересованными сторонами, а также пересматриваться через запланированные интервалы времени и в случае возникновения существенных изменений.
A.5.2	Роли и обязанности в области информационной безопасности	Роли и обязанности в области информационной безопасности должны быть определены и распределены в соответствии с потребностями организации.
A.5.3	Распределение обязанностей	Конфликтующие обязанности и конфликтующие сферы ответственности должны быть разделены.
A.5.4	Обязанности руководства	Руководство должно требовать от всего персонала соблюдения требований информационной безопасности в соответствии с установленной политикой информационной безопасности, конкретными политиками и процедурами организации.
A.5.5	Взаимодействие с соответствующими органами	Организация должна установить и поддерживать контакт с соответствующими органами.
A.5.6	Контакты с группами по интересам	Организация должна устанавливать и поддерживать контакты с специализированными группами или иными форумами специалистов по информационной безопасности и профессиональными ассоциациями.

Внутренние коммуникации

Предмет	Требования НПА, ЛНПА
Когда	В случае, приема/увольнения на работу, в случае изменения требований
С кем	Работники
Кто	Отдел кадров
Процесс	Доведение требований под роспись

Предмет	Информация по обнаруженным несоответствиям
Когда	При обнаружении
С кем	Руководство компании
Кто	Внутренний аудитор
Процесс	В соответствии с процедурой вн. аудита

10. Улучшение

- 10.1 Несоответствия и корректирующие действия
- 10.2 Постоянное улучшение

ISO/IEC 27001:2013

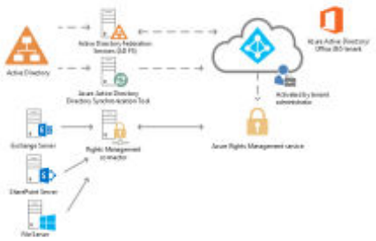
- 10.1 Continual improvement
- 10.2 Nonconformity and corrective action

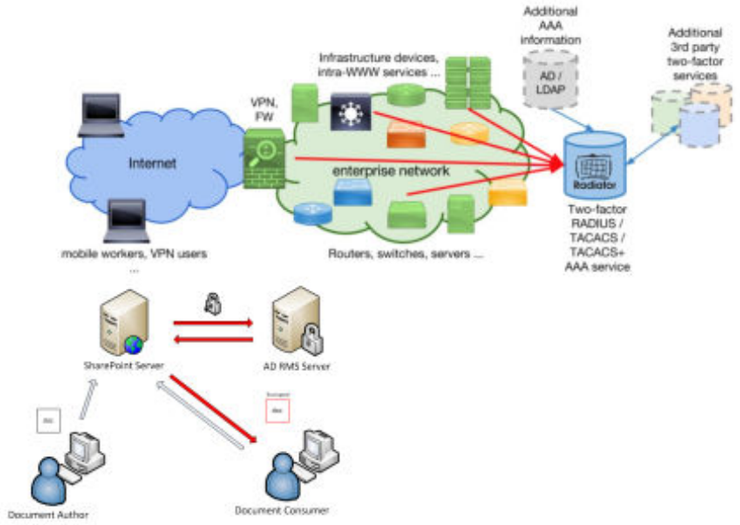
ISO/IEC 27001:2022

ISO/IEC 27001

Управление доступом

- Active Directory (RMS)
- Lightweight Directory Access Protocol (LDAP)
- Terminal Access Controller Access Control System (TACACS)
- Remote Authentication in Dial-In User Service (RADIUS)





ISO/IEC 27001

Физическая безопасность

Организация пропускного режима

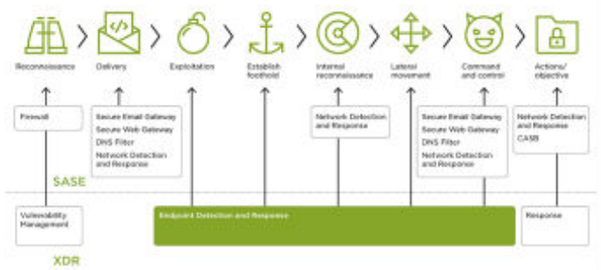
ISO/IEC 27001

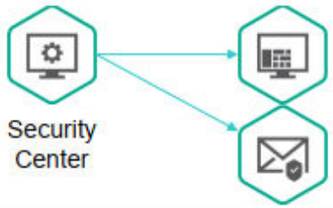
Защита от вредоносных программ

Эшелонированная защита

Мультивендорность

- Файловый антивирус
- Потоковый антивирус
- Почтовый антивирус
- Endpoint Detection & Response (EDR)





Security Center

Endpoint Security for Linux

Secure Mail Gateway

Advanced Malware Protection
NGFW

ISO/IEC 27001

Резервное копирование

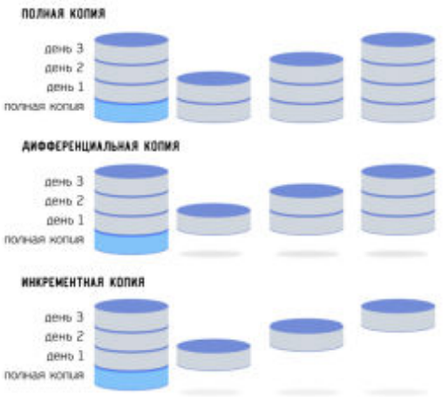
- Данные
- Конфигурации
- Журналы событий
- Виртуальные машины

6.4 Обеспечение резервного копирования пользовательских виртуальных машин

7.5 Определение состава и содержания информации, подлежащей резервированию

7.6 Обеспечение резервирования информации, подлежащей резервированию

7.7 Обеспечение резервирования конфигурационных файлов сетевого оборудования



ISO/IEC 27001

Безопасность сети

- Сегментация
- Управление сетевыми потоками
- NIDS

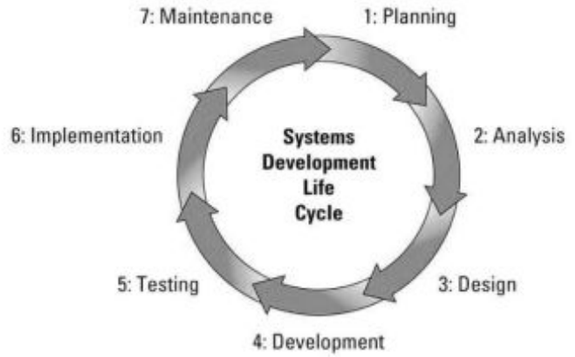
Destinations

Sources	Company Database	Public Cloud	External Partner	Internet
Guest	Deny	Deny	Deny	Permit
Employee BYOD	Permit	Define Access	Deny	Web Apps
Building Mgmt.	Permit	Deny	Deny	Deny
Employee	Permit	Permit	Define Access	Permit

Карта сети

ISO/IEC 27001

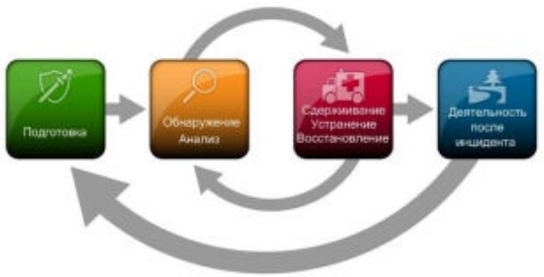
Приобретение, разработка и сопровождение систем



1. Общие положения
2. Список терминов и определений
3. Перечень сокращений
4. Основные положения по обеспечению ИБ
4.1 Обеспечение ИБ на стадиях разработки технических заданий, проектирования, создания и тестирования
4.2 Обеспечение ИБ на стадии приемо-сдаточных испытаний, ввода в опытную эксплуатацию
4.3 Обеспечение ИБ на стадии промышленной эксплуатации (сопровождения и модернизации)
4.4 Обеспечение ИБ на стадии вывода из эксплуатации
5. Контроль за соблюдением требований
6. Ответственность за несоблюдение требований
7. Заключительные положения

ISO/IEC 27001

Управление инцидентами в области информационной безопасности



ISO/IEC 27001

Управление инцидентами в области информационной безопасности

Подготовка.
- Подготовка к обработке инцидентов.
- Предотвращение инцидентов.

Обнаружение и анализ.
- Векторы атаки.
- Признаки инцидента.
- Источники предшественников и индикаторов.
- Анализ инцидента.
- Документирование инцидента.
- Приоритезация инцидента.
- Уведомление об инциденте.

Сдерживание, устранение и восстановление.
- Выбор стратегии сдерживания.
- Сбор и обработка доказательств.
- Идентификация атакующего.
- Устранение и восстановление.

Деятельность после инцидента.
- Полученные уроки.
- Использование собранных по инцидентам данных.

Security Standards Council

Standard: PCI Data Security Standard (PCI DSS)
Version: 1.1
Date: September 2017
Author: Penetration Test Guidance Special Interest Group
PCI Security Standards Council

Information Supplement:
Penetration Testing Guidance

https://www.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf

Methodology

4.1 Pre-Engagement

- 4.1.1 Scoping
- 4.1.2 Documentation
- 4.1.3 Rules of Engagement
- 4.1.4 Third-Party-Hosted / Cloud Environments
- 4.1.5 Success Criteria
- 4.1.6 Review of Past Threats and Vulnerabilities
- 4.1.7 Avoid scan interference on security appliances

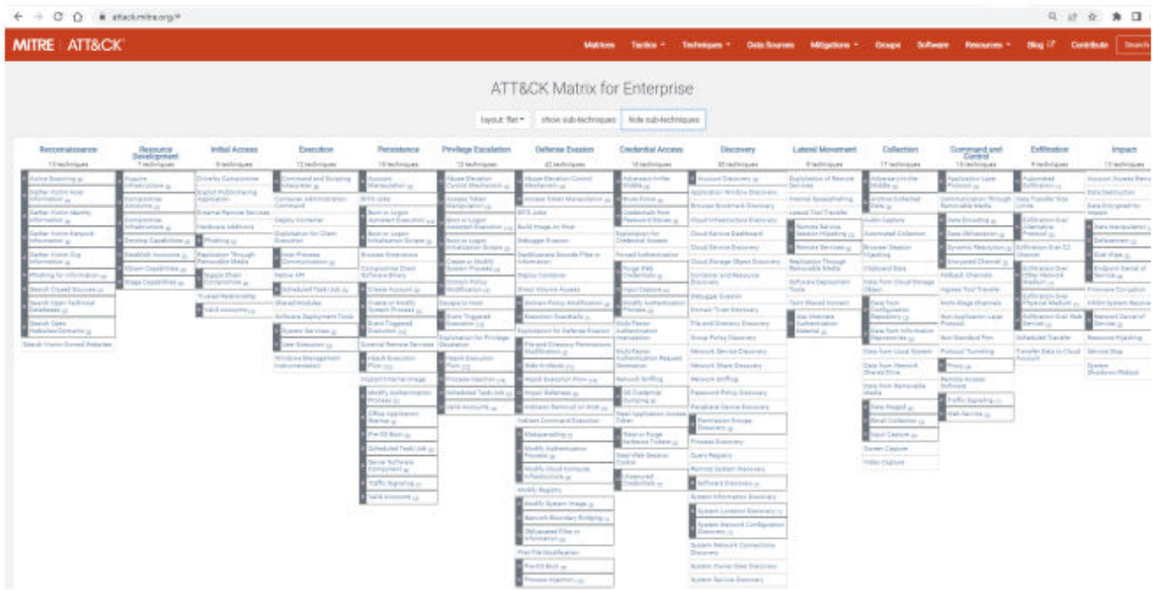
4.2 Engagement: Penetration Testing

- 4.2.1 Application Layer
- 4.2.2 Network Layer
- 4.2.3 Segmentation
- 4.2.4 What to do when cardholder data is encountered
- 4.2.5 Post-Exploitation

4.3 Post-Engagement

- 4.3.1 Remediation Best Practices
- 4.3.2 Retesting Identified Vulnerabilities
- 4.3.3 Cleaning up the Environment

	DETECT	DENY	DISRUPT	DEGRADE	DECEIVE	CONTAIN
RECONNAISSANCE	Web analytics NIDS	NIPS			Disinformation actions Honeypot	
WEAPONIZATION	Threat intelligence					
DELIVERY	Security awareness Endpoint protection NIDS	Anti-spam mechanisms NIPS	Inline AV	Queues	Honeypot	Application firewall Router ACLs
EXPLOITATION	SIEM Security awareness Endpoint protection	Anti-virus HIPS Patch management	DEP			Application firewall Router ACLs
INSTALLATION	NIDS Endpoint protection	HIPS certificates of executable files Two-factor authentication	Privilege situation	Containerisation		Application firewall Router ACLs
COMMAND AND CONTROL	NIDS	IPS	Router ACLs		DNS sinkholes	Network segmentation
ACTION ON OBJECTIVES	SIEM DLP			DLP		Data encryption DLP



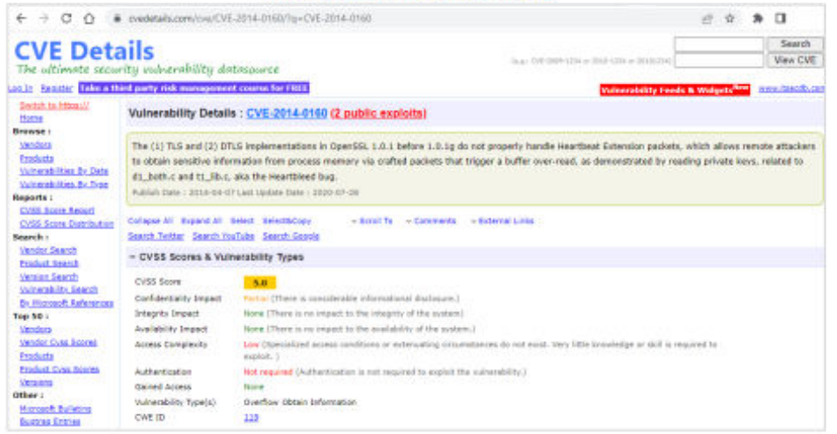
Common Vulnerabilities and Exposures (CVE)

Список стандартных названий для общеизвестных уязвимостей. Основное назначение CVE - это согласование различных баз данных уязвимостей и инструментов, использующих такие базы данных. Поддержку CVE осуществляет MITRE Corporation (www.mitre.org).

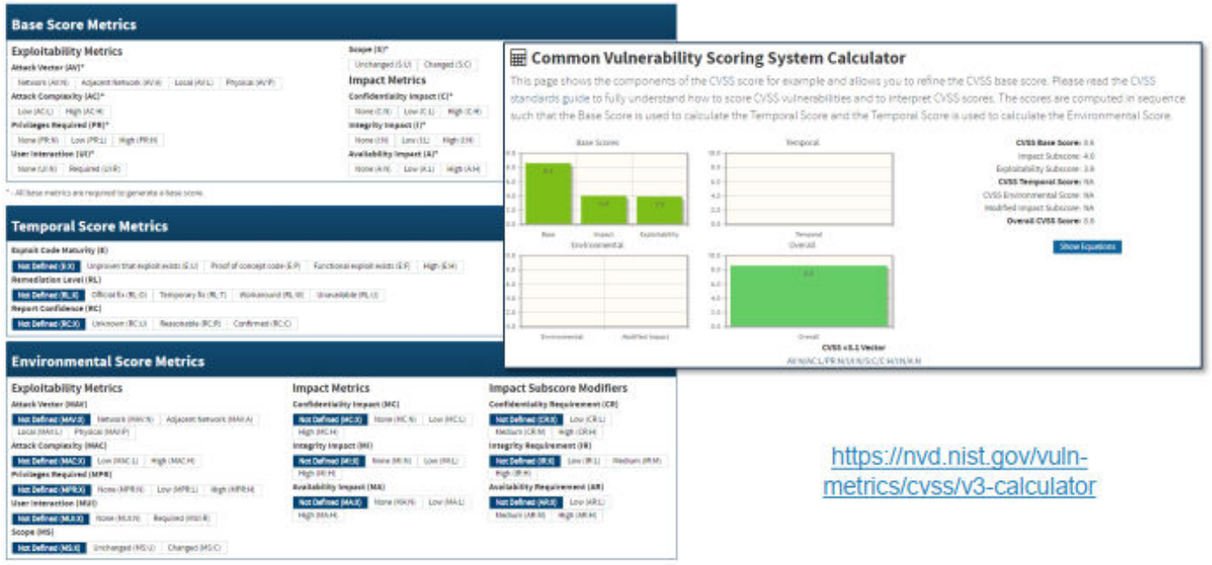
https://www.cvedetails.com/

Heartbleed (CVE-2014-0160) — ошибка в криптографическом программном обеспечении OpenSSL, позволяющая несанкционированно читать память на сервере или на клиенте, в том числе для извлечения закрытого ключа сервера.

https://cve.mitre.org/



Common Vulnerability Scoring System (CVSS)

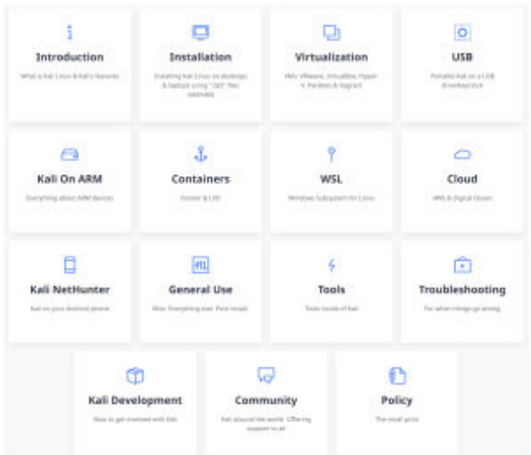


https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

KALI
BY OFFENSIVE SECURITY

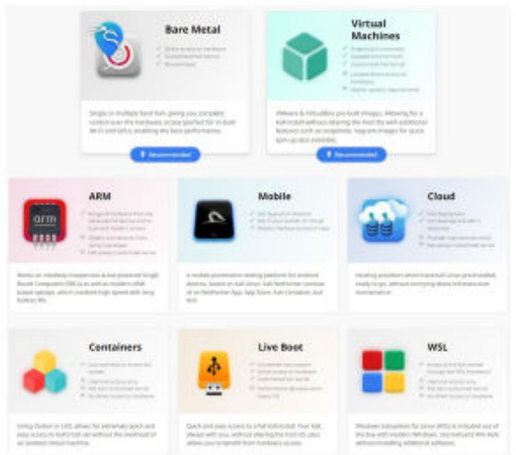
https://www.kali.org/

KALI
BY OFFENSIVE SECURITY



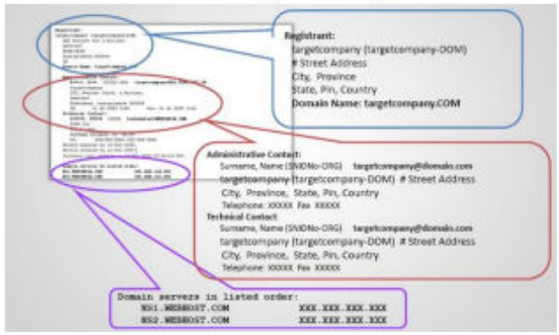
https://www.kali.org/docs/

ДЕМОНСТРАЦИЯ



https://www.kali.org/get-kali/

WHOIS Footprinting



WHOIS Network Footprinting

whois [ip]
Поиск информации об IP адресах и сетевых масках используемых целевой организацией

```
NetRange:       207.142.0.0 - 207.142.255.255
CIDR:           207.142.0.0/16
OriginAS:
NetName:        ALEPON-207-142
NetHandle:      NET-207-142-0-0-1
Parent:         NET-207-0-0-0-0
NetType:        Direct Allocation
Comment:        ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE
RegDate:        1996-06-03
Updated:        2005-02-08
Ref:            http://whois.arin.net/rest/net/NET-207-142-0-0-1

OrgName:        AGIS
OrgId:          AGIS
Address:        1015 31st St NW
City:           Washington
StateProv:      DC
PostalCode:     20007
Country:        US
RegDate:        1994-08-26
Updated:        2005-07-13
Ref:            http://whois.arin.net/rest/org/AGIS

OrgAbuseHandle: COGEN-ARIN
OrgAbuseName:   Cogent Abuse
OrgAbusePhone:  +1-877-875-4311
OrgAbuseEmail:  abuse@cogentco.com
OrgAbuseRef:    http://whois.arin.net/rest/poc/COGEN-ARIN

OrgNOCHandle:  ZC108-ARIN
OrgNOCName:    Cogent Communications
OrgNOCPhone:   +1-877-875-4311
OrgNOCEmail:   noc@cogentco.com
OrgNOCRef:     http://whois.arin.net/rest/poc/ZC108-ARIN

OrgTechHandle: IPALL-ARIN
OrgTechName:   IP Allocation
OrgTechPhone:  +1-877-875-4311
OrgTechEmail:  ipalloc@cogentco.com
OrgTechRef:    http://whois.arin.net/rest/poc/IPALL-ARIN

RTechHandle:  IPALL-ARIN
RTechName:    IP Allocation
RTechPhone:   +1-877-875-4311
RTechEmail:   ipalloc@cogentco.com
RTechRef:     http://whois.arin.net/rest/poc/IPALL-ARIN
```

КАТЕГОРИЯ «РИСК»

«Это вероятность того, что произойдет некое [плохое] событие, которое окажет [негативное] влияние на цели [вашего бизнеса]»

ВИДЫ РИСКА (Банк)

- Кредитный риск
- Страновой риск
- Рыночный риск
- Процентный риск банковского портфеля
- Риск ликвидности
- Операционный риск
- Стратегический риск
- **Репутационный риск**
- Риск концентрации

- **Правовой риск**
- **Кибер-риск**
- **Риск технический**
- **Риск в сфере информационных технологий**
- **Риск, связанный с аутсорсингом**
- **+ еще 13 видов операционного риска**

https://www.nbrb.by/legislation/documents/PP_550_2016.pdf

Процесс управления риском

ISO 31000:2018 «Risk management – Guidelines»

ФАКТОРЫ И ПРИЧИНЫ РИСКА

Факторы риска – условия, способствующие проявлению причин риска.

- ✓ Определяют возникновение причин и воздействие различных видов риска.

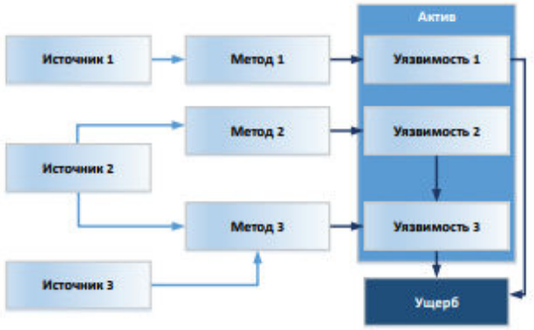
Причина – источник возникновения риска.

- ✓ Конкретные незапланированные события, которые потенциально могут осуществиться и привести к отклонению от намеченного результата.

УГРОЗЫ НАРУШЕНИЯ ИБ

Моделирование

- ✔ Угроза
- ✔ **Источник – Модель нарушителя**
- ✔ Метод реализации
- ✔ **Актив – Классификация в соответствии с НПА, ТНПА**
- ✔ Уязвимость
- ✔ Вероятность
- ✔ Ущерб



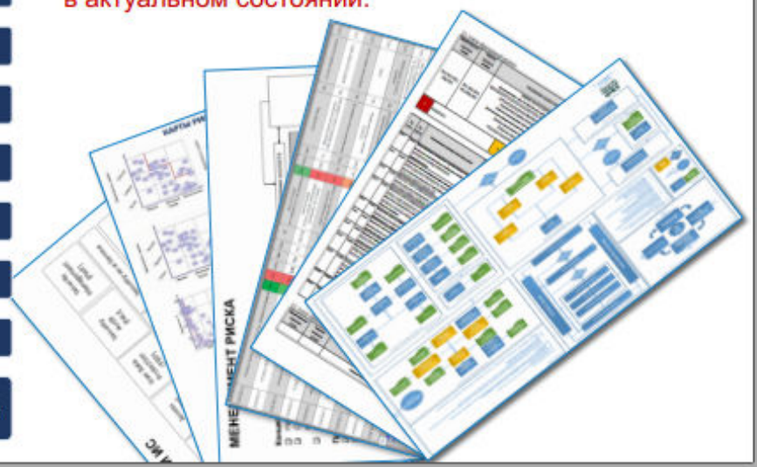
http://bdu.fstec.ru/threat

ISO/IEC 27005 **ТТП 4.1 2020**

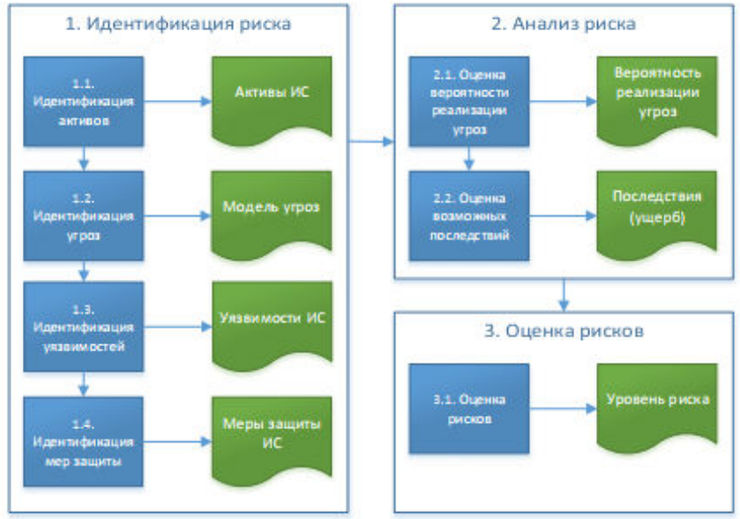
Управление риском нарушения ИБ

- Методика оценки риска
- Реестр информационных активов
- Каталог угроз
- Каталог уязвимостей
- Сценарии реализации риска
- Отчет по результатам оценки риска
- Каталог реализованных мер защиты.
- План обработки риска
- Положение о применимости (свидетельства соответствия требованиям законодательства и стандартов)

Оценка риска это **ПРОЦЕСС** а не проект.
Все документы необходимо поддерживать в актуальном состоянии.



Алгоритм оценки риска (методика)



Оценка риска (качественная / количественная)

Вероятность возникновения угрозы		Низкая			Средняя			Высокая		
Уязвимость актива		Н	С	В	Н	С	В	Н	С	В
Ценность актива	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

SLE = Ценность актива x EF (Exposure Factor)

ALE = SLE x ARO

Воздействие на бизнес (Ущерб)

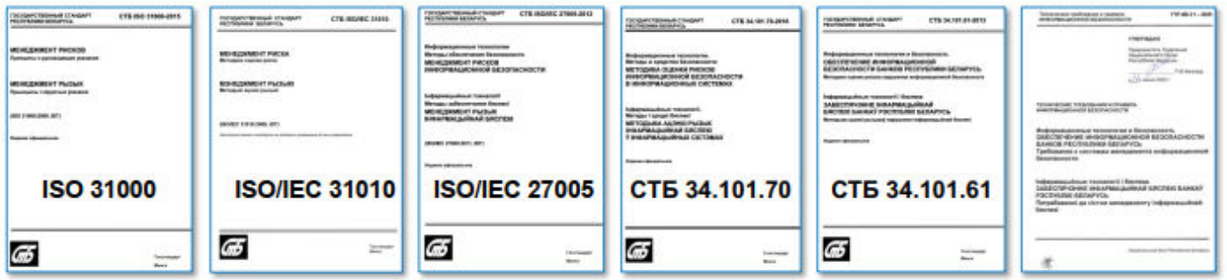
Вероятность	Критический	Высокий	Средний	Низкий	Незначительный
Очень высокая	100%	80%	60%	25%	1%
Высокая	80%	64%	30%	20%	1%
Средняя	60%	30%	38%	16%	1%
Низкая	25%	20%	16%	8%	0%
Очень низкая	1%	1%	1%	0%	0%

SLE – Single Loss Expectancy

ALE – Annualized Loss Expectancy

ARO – Annualized Rate of Occurrence

ПОДХОДЫ К ОЦЕНКЕ РИСКА



Фреймворк моделирования угроз STRIDE

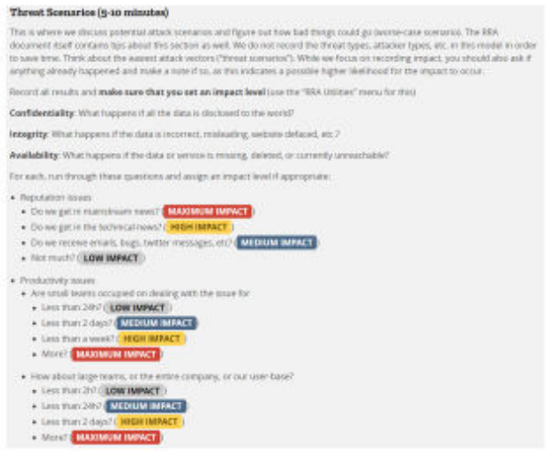
	Угроза	Нарушенное свойство	Пример
S	Spoofing (Спуфинг)	Подлинность	незаконное получение доступа и использование данных аутентификации другого пользователя, например имени пользователя и пароля
T	Tampering (Вмешательство в данные)	Целостность	незаконное внесение изменений в данные, которые, предположим, находятся в базе данных. изменение данных во время их передачи одним компьютером другому по сети.
R	Repudiation (Отрицание)	Неотказуемость	угрозы отрицания исходят от пользователей, которые отрицают выполнение действия, пока другая сторона не докажет обратное
I	Information disclosure (Раскрытие информации)	Конфиден-циальность	предоставление информации тем, кто не должен был получить к ней доступ, например чтение пользователем файла, к которому он не должен иметь доступа, или возможность чтения атакующим данных, передающихся между двумя компьютерами
D	Denial of Service (Отказ в обслуживании)	Доступность	DoS-атаки делают сервисы недоступными для действительных пользователей, например, при временном отсутствии доступа или невозможности использования.
E	Elevation of Privilege (Расширение прав доступа)	Авторизация	получение непривилегированным пользователем расширенных прав доступа и возможностей для вторжения или разрушения всей системы

https://en.wikipedia.org/wiki/STRIDE_(security)

Фреймворк моделирования угроз DREAD

https://en.wikipedia.org/wiki/DREAD_(risk_assessment_model)

Быстрая оценка рисков



https://infosec.mozilla.org/guidelines/risk/rapid_risk_assessment

https://docs.google.com/document/d/1QMRdBLIQYqbn5lMmrOIBwS55Yh9fIYNp4dO3-HMyiyk/edit

ТТП ИБ 2.1 «Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Требования к системам менеджмента информационной безопасности».

ТТП ИБ 2.1-2020

8 Требования к выбору/коррекции подхода к оценке рисков нарушения информационной безопасности и проведению оценки рисков нарушения информационной безопасности

9 Требования к разработке планов обработки рисков нарушения информационной безопасности

Постановление правления **НБРБ № 550** «Инструкция об организации системы управления рисками ...»

ТТП 1.1 - 2020

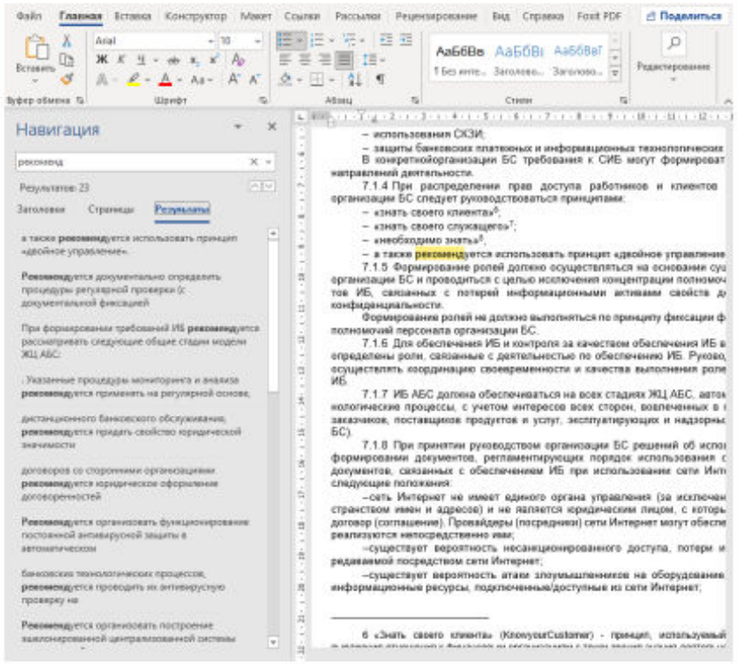
Содержание

5 Исходная концептуальная схема (парадигма) обеспечения ИБ организаций БС

6 Модели угроз и нарушителей информационной безопасности организации БС

7 Система информационной безопасности организаций БС

8 Проверка и оценка информационной безопасности организации БС



ТТП 4.1 - 2020

Свойства

ПРИМЕРНАЯ ФОРМА ДОКУМЕНТИРОВАНИЯ ПЕРЕЧНЯ ТИПОВ ИНФОРМАЦИОННЫХ АКТИВОВ ОБЛАСТИ ОЦЕНКИ РИСКОВ НАРУШЕНИЯ ИБ И ИХ СВОЙСТВ ИБ

На примере заполнения:
тип информационного актива –«Служебная информация ограниченного распространения» (далее – «ДСП информация»).

Тип информационного актива	Свойства информационной безопасности			
	конфиденциальность	целостность	доступность	другие свойства ИБ (при необходимости)
«ДСП информация»	+	+	+	-
...				
...				

Примечание:
Свойства ИБ, поддержание которых необходимо обеспечивать в рамках СОИБ организации БС для типа информационного актива, обозначаются знаком «+», остальные свойства ИБ - знаком «-».

ТТП 2.1 - 2020

Документирование и рекомендации