МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**



**МОСКОВСКИЙ**

**ПОЛИТЕХ**

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Кафедра «Информационная безопасность»

Проектная деятельность

Тема: “Оценка зрелости фреймворка **CIS Critical Security Controls**”

Выполнил: Студент 2 курса гр. 191-331

Юрин Даниил Романович

Научный руководитель:

Агеева Елена Александровна

2020 г. Москва

**Содержание:**

Вступление………………………………………………………………………..2

Этап 1: Модель CIS Controls V7……………….………………………………...4

Этап 1: Элементы управления безопасностью……….…………………………7

Вывод………………………………………………………………………………9

**Вступление:**

Информационная безопасность компании, общественной организации или производственного предприятия – это комплекс мероприятий, направленных на предотвращение несанкционированного доступа к внутренней IT-инфраструктуре, незаконного завладения конфиденциальной информацией и внесения изменений в базы данных. [Википедия](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C) включает в это понятие любые формы данных, независимо от их материального представления. То есть, в информационную безопасность входит защита от злоумышленников данных в электронной форме и на физических носителях.

Учитывая важность информации в современном мире, защите от утечек конфиденциальной информации в адрес конкурентов необходимо уделять повышенное внимание. Возможный ущерб может быть намного большим, чем стоимость всех материальных активов предприятия. Именно поэтому, современные организации используют специальные фреймворки по защите своих данных.

Существует множество различных фреймворков, предоставляемых на рынке защиты информации, но самый известный из них - это **CIS Controls V7**. Принцип работы которого мы сейчас и рассмотрим.

**Этап 1.**

**Модель CIS Controls V7.**

Модель «**CIS Critical Security Controls**», была разработана ведущими экспертами института **SANS**, объединившими свои колоссальные знания и навыки в области кибербезопасности.

Они создали обширный список средств контроля данных в интернете, представляющий собой лучшие методы защиты от киберпреступности.

Данные методы гарантируют, что средства управления **CIS** являются наиболее эффективными мерами защиты, обеспечивающими сохранность данных компаний, как от наиболее известных и распространенных кибератак в сети, так и от самых сложных и менее популярных способов кражи.

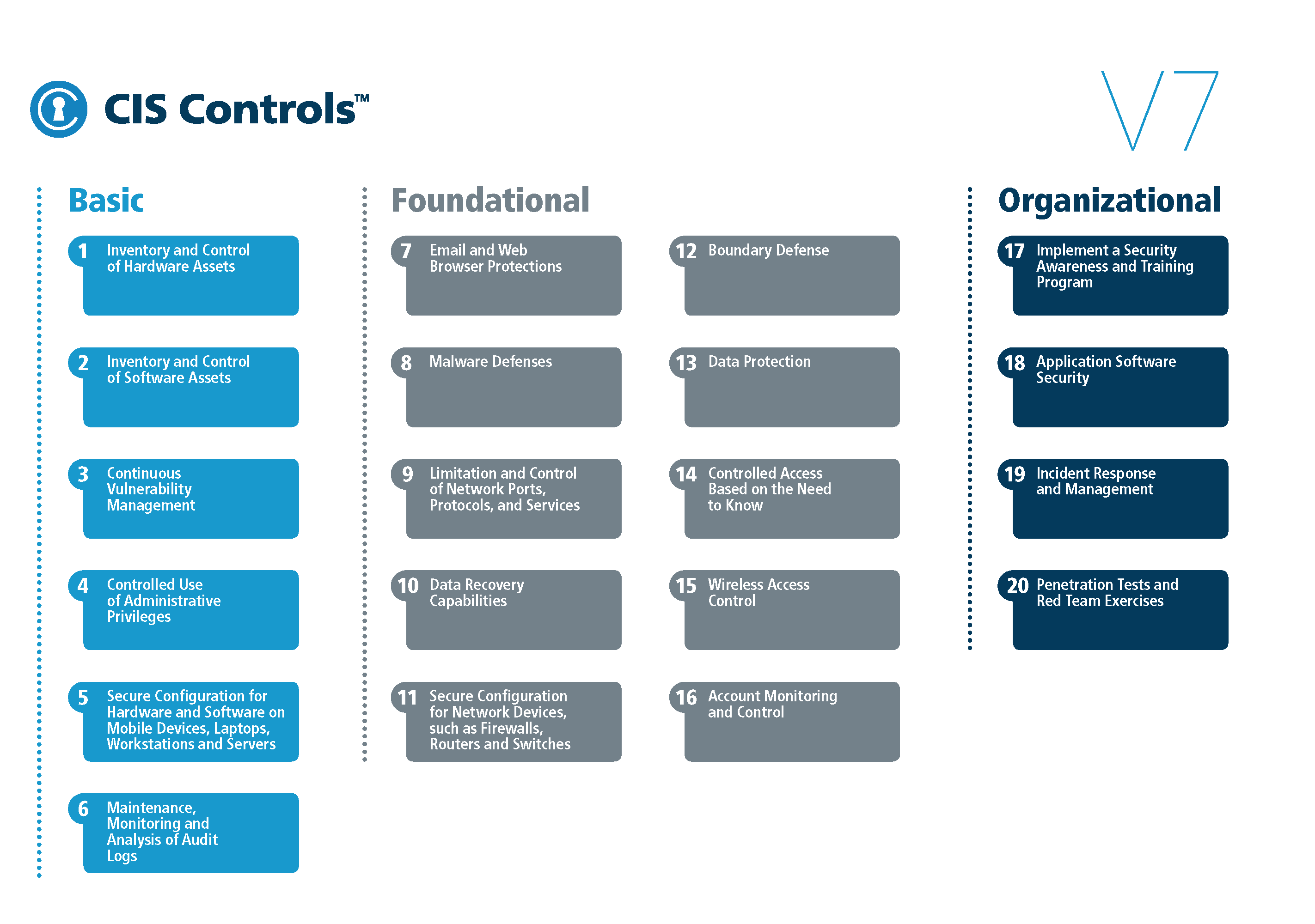
Для этого **CIS** разработало **пять** важнейших принципов работы эффективной системы киберзащиты:

1. **Offense informs defense (**Нападение информирует защиту**).** Суть этого принципа заключается в том, что используются знания о реальных атаках, произведённых на системы. Это нужно для того, чтобы обеспечить эффективность работы средств защиты.
2. **Prioritization** (Определение приоритетов). Суть данного принципа заключается в том, что сначала устанавливаются те средства управления системой, которые смогут обеспечить максимальное снижение рисков потери данных от наиболее опасных угроз. Помимо этого, происходит установка только тех систем, которые могут быть реально реализованы в вашей вычислительной среде. Не нужно тратить средства на те системы, которые не принесут максимальную защиту от киберугроз и не смогут корректно работать в вашей среде.
3. **Measurements and Metrics** (Измерения и метрики). Суть этого принципа заключается в том, что устанавливаются единые показатели, чтобы руководители, ИТ-специалисты, аудиторы и сотрудники службы безопасности использовали общий язык для измерения эффективности мер безопасности в организации. Это нужно для того, чтобы можно в дальнейшем легко производить необходимые корректировки в системе.
4. **Continuous diagnostics and mitigation** (Непрерывная диагностика и устранение неполадок). Суть данного принципа заключается в том, что все время должно выполняться непрерывное тестирование эффективности работы текущих мер защиты и обеспечения безопасности.
5. **Automation** (Автоматизация). Суть данного принципа заключается в том, что производится автоматизация средств защиты.

Помимо этого, **CIS** разделило меры защиты от кибератак на специальные группы реализации **IG1**, **IG2,** **IG3**:

* [](https://4.bp.blogspot.com/-_8xUuNXmfTM/XKsR4J4vmSI/AAAAAAAAa5Y/SvXhgUooVawGDEuviejMUKmVDbhCkVyfgCLcBGAs/s1600/IG1.png)**Implementation group 1 - IG1.** Организации, применяющие **IG1** – в основном малый (иногда средний бизнес), с ограниченным опытом в ИТ и кибербезопасности. Основная задача этих организаций - сохранить бизнес в рабочем состоянии, а основной ущерб - от простоя.  Как правило обрабатывают не критичные данные своих сотрудников и финансовую информацию. Если же организации малого бизнеса обрабатывают критичные данные, то должны выполнять меры следующих групп. Меры защиты, реализуемые в рамках группы **IG1**, должны осуществляться в варианте, требующем минимум компетенций в области ИБ и рассчитаны на коробочные решения оборудования и ПО для малого бизнеса.
* [](https://3.bp.blogspot.com/-w380mOVKrzU/XKsR4FLUFiI/AAAAAAAAa5U/9F2bU7sO14EZ2U8KKkUtGLtzMA9BpXsagCLcBGAs/s1600/IG2.png)**Implementation group 2 – IG2.** В организациях, применяющих **IG2** как правило есть выделенные работники, отвечающие за управление ИБ и защиты ИТ инфраструктуры. В таких организациях есть процессы и подразделения разной степени критичности. Некоторые подразделения могут быть нацелены в первую очередь на выполнение требований законодательства (**compliance**). Организации группы **IG2** как правило обрабатывают важную информацию своих клиентов и контрагентов и устойчивы к коротким перерывам в обслуживании. Основное беспокойство вызывает потеря репутации в случае инцидентов. Частные меры группы **IG2**, помогают ответственным за безопасность лицам, справляться с возрастающей сложностью процессов и операций. Установки и настройки некоторых меры будут зависеть от имеющегося в компании уровня технологий и экспертизы.
* [https://1.bp.blogspot.com/-_p372dmE1dY/XKsR4H724mI/AAAAAAAAa5c/-enwRSA72bMsjQxMhYMBvrALwj5k0mwDQCLcBGAs/s200/IG3.png](https://1.bp.blogspot.com/-_p372dmE1dY/XKsR4H724mI/AAAAAAAAa5c/-enwRSA72bMsjQxMhYMBvrALwj5k0mwDQCLcBGAs/s1600/IG3.png)**Implementation group 3 – IG3.** В организациях группы **IG3** тысячи работников, в том числе имеются эксперты по безопасности, которые специализируются на различных аспектах кибербезопасность (например, управление рисками, тестирование на проникновение, безопасность приложений). Системы и данные организаций группы **IG3** содержат конфиденциальную информацию или функции, которые строго регулируются или должны соответствовать требованиям. Организации группы **IG3** должны обеспечивать доступность услуг, конфиденциальность и целостность данных. Успешные атаки могут нанести большой вред обществу. Меры защиты, выбранные для **IG3**, направлены на противодействие целевым и новым атакам от нарушителей с высоким потенциалом.

**Элементы управления безопасностью.**

Описание критических элементов управления безопасностью включает в себя всесторонние проверки элементов ИТ-инфраструктуры, конфигураций, прав доступа, привилегий, системных журналов, мер и средств реагирования на инциденты и инициирование проверок.  
В 7 редакции руководства элементы распределены на три категории, учитывающие современный ландшафт киберугроз.  


**Базовые.**  
В этой категории содержатся рекомендации, необходимые для обеспечения информационной безопасности организации. В эту категорию входят следующие пункты:

* инвентаризация авторизированных и неавторизованных устройств;
* инвентаризация авторизированного и неавторизованного программного обеспечения;
* средства управления уязвимостями;
* использование административных привилегий;
* защищенные конфигурации для мобильных устройств, ноутбуков, АРМ и серверов;
* обслуживание, мониторинг и анализ журналов аудита.

**Фундаментальные.**  
В эту категорию входят рекомендации, необходимые для применения лучших практик для обеспечения преимуществ и использования передовых технологий кибер-безопасности. В эту категорию входят следующие пункты:

* защита электронной почты и веб-браузера;
* защита от вредоносных программ;
* ограничение и контроль сетевых портов;
* возможность восстановления данных;
* защищенные конфигурации для сетевых устройств;
* защита периметра;
* защита данных;
* контроль доступа;
* контроль доступа беспроводных сетей;
* контроль учетных записей.

**Организационные**.  
В эту категорию входят рекомендации, ориентированные на организационные процессы и административные меры, связанные с обеспечением информационной безопасности, с целью повышения осведомленности персонала и проведения Red Team/Blue Team операций. В эту категорию входят следующие пункты:

* контроль уровня осведомленности персонала;
* контроль прикладного программного обеспечения;
* реагирование на инциденты;
* тестирование на проникновение/Red Team.

Эти рекомендации позволяют составить четкие и приоритетные руководства для решения задач по обеспечению информационной безопасности организации и могут быть использованы как основа политик информационной безопасности.

**Вывод.**  
Модель **CIS Controls V7** была разработана для любых типов организаций, коммерческих фирм, неправительственных организаций, производственных предприятий:

* Применима к любой организации независимо от размера, контекста и ресурсов;
* Требует высокой квалификации менеджеров по безопасности и высокой детализации процессов безопасности;
* Позволяет организациям расположить по приоритетам и оптимизировать свои инвестиции в безопасность;