Аннотация – Анализ «Cyber Defense Doctrine Managing the Risk: Full Applied Guide to Organizational Cyber Defense» посвящён различным аспектам организационной киберзащиты, включая системы управления рисками, элементы кибербезопасности в военных операциях, планирование реагирования на инциденты и применение инструментов и методов киберзащиты. Подчёркивая полезность для специалистов по кибербезопасности и специалистов в различных отраслях, изложенный материал можно рассматривать в качестве руководства, которое даёт представление о реализации стратегий киберзащиты, повышении уровня безопасности организации и развитии кибер-культуры.

Он также служит полезным ресурсом для специалистов в области информационных технологий, криминалистики, правоохранительных органов и других секторов, которым требуется глубокое понимание принципов и практик киберзащиты и необходимость непрерывного обучения и адаптации с учётом постоянно развивающихся кибер-угроз.

I. Введение

Ключевые моменты дающие представление о доктрине представлены следующим списком:

- **Цель (основная)**: продвижение киберзащиты в израильской экономике как часть национальных усилий (Израиля) по защите гражданского киберпространства
- **Цель (вторичная)**: предоставление системного профессионального метода управления кибер-рисками в организациях, распознавания соответствующих рисков, формулирования защитных мер и реализации плана снижения рисков.
- **Категории организаций:** различение двух типов организаций в зависимости от размера потенциального ущерба от кибер-инцидента.
- **Процесс оценки и управления рисками:** различные методы оценки и управления рисками, в зависимости от размера организации, соответствия законодательным и нормативным требованиям и других параметров (например, с небольшим потенциалом ущерба до 1,5 млн долларов и более).
- **Результат:** понимание карты организационных рисков и то, какие меры контроля необходимы для снижения этих рисков; которые (меры) станут основой для построения плана работы, распределения ресурсов и подготовки организации.
- **Принципы доктрины:** ответственность управления, защита с точки зрения противника, защита, основанная на израильских знаниях и опыте, защита в соответствии с потенциалом ущерба.

II. Принципы доктрины

Целью является формирование принципов, которых организациям следует придерживаться, чтобы эффективно управлять кибер-рисками и повышать свою кибер-устойчивость.

Целевая аудитория включает руководителей организаций, специалистов по информационной безопасности и экспертов по киберзащите, которые отвечают за управление кибер-рисками и реализацию стратегий защиты в своих организациях.

A. Процесс автоматизации и интеграции

Подчёркивается важность процессов автоматизации и интеграции:

- Процессы автоматизации снижают необходимость участия человека в защитных и операционных процессах, тем самым сводя к минимуму вероятность человеческой ошибки.
- Внедрение MITRE ATT&CK с целью использования передовых автоматизированных решений для непрерывного контроля и реализации процессов реагирования минимизирует объём ручного участия человека.
- Применение превентивных мер сохранения информации, включая поддержание эффективных возможностей реагирования на случаи утечки информации, например получение возможности удалять информацию, которая попала в Интернет и даркнет.
- Директор по информационной безопасности (CISO) играет важную роль в защите информации и конфиденциальности и должен использовать различные инструменты для максимизации уровня защиты.
- Средства контроля доктрины включены в систему, включающую аспекты идентификации, защиты, обнаружения, реагирования и восстановления.

- Концепция защиты, необходимая для борьбы с современными угрозами поможет организации достичь новых возможностей с целью выиграть время, измотать злоумышленника и даже создать факторы сдерживания против злоумышленников.

B. Роль директора по информационной безопасности

Директор по информационной безопасности играет решающую роль в защите информации и конфиденциальности внутри организации. Это включает в себя понимание и соблюдение мер конфиденциальности, баланса различных интересов, управление рисками, разработку стратегий защиты и эффективное внедрение средств контроля:

- **Закон о защите конфиденциальности**: любое посягательство на неприкосновенность частной жизни должно осуществляться в соответствии с законом и общими принципами разумности и добросовестности
- **Баланс интересов:** Директор по информационной безопасности должен найти правильный баланс между различными интересами, чтобы обеспечить обоснованные решения внутри организации. Это включает в себя рассмотрение аспектов конфиденциальности и соблюдение таких принципов, как «Security by Design», «Privacy by Design» и защита с учётом угроз.
- **Оценка и управление рисками:** процесс оценки и управления рисками включает определение основных целей защиты, выявление пробелов в защите и построение плана работы по минимизации этих пробелов.
- **Ответственность руководства:** Ответственность за защиту информации в первую очередь лежит на руководстве организации и директор по ИБ является ключевой фигурой в обеспечении выполнения этой обязанности.
- **Защита с точки зрения противника:** Директор по информационной безопасности должен понимать распространённые сценарии атак и эффективность рекомендаций по защите от них. Это понимание определяет вес и приоритет рекомендаций защиты.
- **Защита, основанная на потенциальном ущербе:** инвестиции в защиту каждой цели защиты должны соответствовать уровню её критичности для функционирования организации. Директор по информационной безопасности должен управлять этими инвестициями
- **Организационная классификация:** классификации основана на потенциальном ущербе от кибер-инцидента. Директор по информационной безопасности должен понимать место организации для формирования стратегий защиты.

III. ПРОЦЕСС ПЛАНИРОВАНИЯ С ТОЧКИ ОРГАНИЗАЦИИ

Процесс планирования с точки зрения организации — это метод управления рисками внутри организации. Цель этого процесса — помочь организациям выявить соответствующие риски, сформулировать защитные меры и соответствующим образом реализовать план снижения рисков.

Целевая аудитория включает менеджеров и экспертов в области информационной безопасности и киберзащиты.

Применяются различные методы оценки и управления рисками, в зависимости от размера организации, соответствия законодательным и нормативным требованиям и другими параметрами. Например, к организациям категории А относятся организации, у которых объем ущерба, причинённого кибер-инцидентом, не превышает 1,5 млн долларов США, а к организациям категории Б – организации, у которых размер ущерба, причинённого кибер-инцидентом, может стоить более 1,5 млн долларов США.

Для организаций категории А применяется простой и быстрый процесс определения целей защиты, специально предназначенных для организаций этой категории.

Для организаций категории В применяется не только процесс оценки рисков, но понимание необходимых мер защиты по матрице рисков и склонности к риску, изучение текущей ситуации с точки зрения принятых в отрасли рекомендаций по защите и формулирование плана работы для снижения рисков.

Конечный результат работы заключается в том, что организация определяет карту организационных рисков и то, какие средства контроля необходимы для снижения этих рисков, включая правильные приоритеты для реализации плана работы. Эти средства контроля станут основой для построения плана работы, распределения ресурсов и соответствующей подготовки организации.

A. Ключевые компоненты процесса планирования

Ключевые компоненты процесса планирования в организации включают:

- **Разграничение деятельности:** понимание цифровых активов организации и места их хранения для определения подлежащего защита набора объектов.
- **Оценка рисков:** выявление соответствующих рисков для организации, анализ этих рисков и их оценка для понимания их потенциального воздействия и вероятности.
- **Управление риском:** принятие решения о стратегии борьбы с выявленными рисками
- **Построение плана работы:** после того как риски идентифицированы и определена стратегия борьбы с ними, организация должна разработать план работы по устранению рисков. Этот план может

включать внедрение процессов, приобретение решений и обучение сотрудников.

- **Непрерывный аудит и контроль:** реализация плана работы должна регулярно пересматриваться, чтобы гарантировать его эффективность и актуальность. Это включает в себя проверку новых информационных активов, реализованных средств контроля и необходимых управленческих данных.
- **Привлечение юрисконсульта:** юрисконсульт организации должен быть привлечён на ранних стадиях процесса планирования, чтобы обеспечить соблюдение законодательных и нормативных требований и быть интегрированным в ключевые процессы принятия решений.
- **Принятие решений, подкреплённое доказательствами:** организация должна использовать независимых аудиторов и экспертов, чтобы справиться с различными угрозами и гарантировать, что принятие решений подкреплено доказательствами, которые обеспечат реалистичную картину ситуации с безопасностью.
- **Минимизация вторжения в частную жизнь:** Структура управления предлагает директору по ИБ широкую свободу действий для снижения уровня риска до приемлемого значения, одновременно сводя к минимуму вторжение в частную жизнь.

IV. Реализация Доктрины

A. Основные моменты:

- Подчёркивается важность процессов автоматизации и координации для уменьшения человеческих ошибок и воздействия личной информации.
- Поощряется использование передовых автоматизированных решений для непрерывного контроля и выполнения процессов реагирования, при этом участие человека требуется лишь в исключительных случаях.
- Необходимость применения превентивных мер защиты для сохранения информации, а также для поддержания эффективных возможностей реагирования на случаи утечки информации.
- Средства контроля доктрины включены в структуру, включающую аспекты идентификации, защиты, обнаружения, реагирования и восстановления.
- Необходимость внедрения средств контроля на разных уровнях зрелости по таким вопросам, как SOC, DLP или исследования рисков.
- Сосредоточение внимание на рисках, актуальных для каждой организации, при этом периодические проверки и разведывательные оценки проводятся по всей израильской экономике.
- Инвестиции в защиту каждого объекта защиты в организации будут соответствовать уровню его критичности для функционирования организации.

B. Разница контроля уровня

Контроль базового уровня обычно указывает на процесс, который существует, но не управляется и выполняется вручную. Это отправная точка для организаций, позволяющая им внедрить базовые элементы управления, прежде чем переходить к более продвинутым и сложным элементам управления.

С другой стороны, контроль инновационного уровня означает реализацию контроля управляемым, документированным, автоматическим, эффективным и действенным образом. Этот уровень контроля является более комплексным и учитывает ограничения организации, классификацию информации и адаптацию к бизнес-процессам.

V. Реализация Доктрины для организации категории А

В случае организаций категории А рассматривается пятиэтапный процесс реализации доктрины.

- **Этап 1: Разграничение деятельности.** этап включает определение объёма деятельности организации, которую необходимо защитить.
- **Этапы 2 и 3: Оценка рисков и определение стратегии борьбы с ними.** этапы включают выявление потенциальных рисков для организации и разработку стратегии управления этими рисками.
- **Этап 4: Составление плана работы.** этап включает в себя создание подробного плана реализации стратегии защиты.
- **Этап 5: Непрерывный аудит и контроль.** этап включает постоянный мониторинг и контроль для обеспечения эффективности стратегии защиты и внесения необходимых корректировок.

VI. Реализация Доктрины для организации категории Б

В случае организаций категории Б рассматривается пятиэтапный процесс реализации доктрины.

- **Этап 0 – Корпоративное управление и стратегия управления корпоративными рисками.** этап включает в себя создание структуры управления и стратегии управления корпоративными рисками. Он закладывает основу подхода организации к киберзащите.
- **Этап 1 – Разграничение деятельности и обследование по оценке рисков.** этап включает в себя определение сферы деятельности организации и проведение обследования по оценке рисков. Это помогает организации понять свои потенциальные уязвимости и риски, связанные с её деятельностью.

- **Этап 2 – Оценка рисков.** этап включает детальную оценку рисков, выявленных на предыдущем этапе. Организация оценивает потенциальное воздействие и вероятность каждого риска, что помогает расставить приоритеты для их смягчения.
- **Этап 3 – Управление риском.** этап включает разработку стратегий по управлению ими: снижение риска, принятие или предотвращение, в зависимости от характера риска и толерантности к риску организации.
- **Этап 4 – Построение плана работы:** на основе стратегий управления рисками, разработанных на предыдущем этапе, этот этап включает в себя создание подробного плана работы, где описываются шаги, которые организация предпримет для реализации своих стратегий управления рисками.
- **Этап 5 – Непрерывный аудит и мониторинг.** этап включает постоянный аудит и мониторинг, чтобы гарантировать эффективную реализацию стратегий управления рисками и выявлять любые новые или изменяющиеся риски.

VII. Структура защиты

Структура представлена следующим образом:

- **Идентификация:** функция включает в себя развитие организационного понимания управления рисками кибербезопасности для систем, активов, данных и возможностей.
- **Защита:** функция определяет соответствующие меры безопасности для обеспечения предоставления критически важных инфраструктурных услуг.
- **Обнаружение:** функция определяет соответствующие действия для выявления возникновения события кибербезопасности.
- **Ответ:** функция включает в себя соответствующие действия для принятия мер в отношении обнаруженного инцидента кибербезопасности.
- **Восстановление:** функция определяет соответствующие действия для поддержания планов устойчивости и восстановления любых возможностей или услуг, которые были нарушены из-за инцидента кибербезопасности.

Эти функции построены в соответствии со структурой кибербезопасности NIST (CSF), которая обеспечивает высокоуровневую классификацию результатов кибербезопасности и методологию оценки этих результатов и управления ими.

VIII. Прочее

Ключевые принципы включают принцип согласия, который даёт клиентам контроль над их личной информацией, и принцип близости цели, который предусматривает, что информация может использоваться только для той цели, для которой она была первоначально собрана. В нем также изложены обязательства относительно регистрации баз данных и их безопасности, включая необходимость периодической проверки необходимости сохранения информации исходя из её первоначальной цели сбора.

A. Средства защиты организации

Ключевые аспекты в контексте мер по контролю за защитой организации категории А:

Требование к доказательствам: подчёркивается необходимость надлежащей документации для обеспечения правильной интеграции средств контроля в организацию. Эти данные также могут служить основой для регулирования и/или аккредитации/сертификации.

Ранжирование и установление приоритетов: элементы управления классифицированы по шкале от 1 до 4. Средства управления уровня 1 являются самыми базовыми и необходимы для любой организации для каждого актива, тогда как элементы управления уровня 4 необходимы только для объекта защиты, потенциальный ущерб которого 4

Непрерывный контроль. Непрерывный контроль позволяет понять, каковы пробелы в защите и какие шаги необходимы для улучшения ситуации. Непрерывный контроль может осуществляться на уровне соответствия, решая определённые проблемы и средства контроля, или путём измерения рисков, угроз, готовности к сценариям атак и т. д.

Ключевые показатели эффективности (KPI): KPI позволяют организации измерять и количественно определять уровень защиты в определённый момент времени, сравнивая его с историей измерений, таким образом исследуя тенденцию.

Процесс оценки и управления рисками. Деятельность по киберзащите осуществляется в связи с желанием организации управлять кибер-рисками, которым она подвергается. Сначала определяются основные цели защиты, требуемый уровень защиты и пробелы в защите по сравнению с желаемой ситуацией, а затем формируется план работы по минимизации пробелов.

Конечный продукт: карта организационных рисков и то, какие средства контроля необходимы для снижения этих рисков в качестве средств контроля являются основой для построения плана работы, распределения ресурсов и соответствующей подготовки организации.