СТРУКТУРНЫЕ ЭЛЕМЕНТЫ КИБЕРБЕЗОПАСНОСТИ В ЭНЕРГЕТИЧЕСКОМ СЕКТОРЕ

Морис Мартин, Тами Рейнольдс, Анудж Сангви, Сэди Кокс и Джеймс Элсворт

Национальная лаборатория по исследованиям в области возобновляемых источников энергии

Март 2021 г.

Подготовлено в рамках Соглашения о партнерстве USAID-NREL № IAG-17-2050

УВЕДОМЛЕНИЕ

Данная работа частично подготовлена Национальной лабораторией по исследованиям в области возобновляемых источников энергии (NREL), находящейся в ведении Альянса за устойчивую энергетику (Alliance for Sustainable Energy, LLC), для Министерства энергетики США (DOE) по Договору № DE-AC36-08GO28308. Финансирование предоставлено Агентством международного развития США (USAID) по Договору № IAG-17-2050. Мнения, выраженные в данном отчете, не обязательно отражают точку зрения DOE, правительства США или любого агентства, включая USAID.

Выражение признательности

Авторы хотели бы поблагодарить Джамилю Амодео с Агентства США по международному развитию, за ее интеллектуальное лидерство и инструментальное руководство при разработке структурных элементов кибербезопасности энергетического сектора а также, за ее тщательное изучение и вклад в эту публикацию.

Перечень сокращений

CEO	руководитель организации
CTI	разведка в области киберугроз
DER-CF	рамки кибербезопасности распределенных энергетических ресурсов
ICS	системы управления производственными процессами
IDS	система обнаружения вторжений
IEC	Международная электротехническая комиссия
ISACS	Центры обмена информацией и анализа
ISO	Международная организация по стандартизации
NIST	Национальный институт стандартов и технологии США
NREL	Национальная лаборатория по исследованиям в области возобновляемых источников энергии
SCADA	контроль технологических и производственных процессов
USAID	Агентство США по международному развитию

Содержание

Перечень рисунков

Перечень таблиц

1 Структурные блоки кибербезопасности в энергетическом секторе

Структурные блоки кибербезопасности, разработанные в рамках Партнерства[1] между Агентством международного развития США (USAID) и Национальной лабораторией по исследованиям в области возобновляемых источников энергии (NREL), а также партнерская Платформа устойчивой энергетики,[2] предназначены для того, чтобы помочь различным заинтересованным сторонам повысить безопасность электросети. Данные работы являются результатом обсуждений между USAID, NREL и энергетическими предприятиями по всему миру, а также предыдущих оценок кибербезопасности, выполненных NREL для десятков энергетических предприятий и государственных учреждений, с акцентом на проблемы кибербезопасности, с которыми сталкиваются небольшие энергетические предприятия с ограниченными ресурсами.

В документе описаны одиннадцать **структурных блоков** кибербезопасности в энергетическом секторе (Рисунок 1). Это своего рода руководство с помощью которого организации могут разработать надежную программу кибербезопасности. По отдельности каждый структурный блок представляет собой группу связанных действий в рамках кибербезопасности, на которых организации следует сосредоточиться. Используя стандартные блоки, организации могут эффективно расставить приоритеты своих работ по кибербезопасности, чтобы наилучшим образом предотвратить широкий спектр потенциальных кибератак.

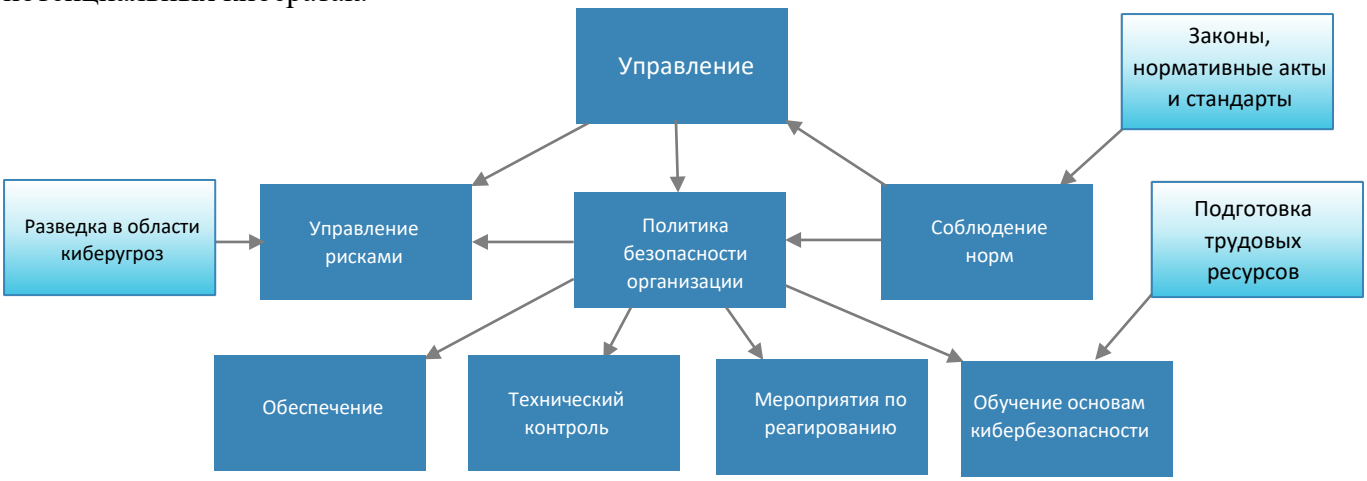


Рисунок 1. Структурные элементы кибербезопасности в энергетическом секторе

Примечание: Блоки, окрашенные сплошной заливкой, являются внутренними для компании, а блоки с градиентом – внешними.

1.1 О структурных блоках

1.1.1 Потребность

Существует множество прекрасных руководств, стандартов и наработок для организаций, стремящихся улучшить свою кибербезопасность. Часть из них была разработана органами стандартизации, такими как Международная организация по стандартизации (ISO). Другие были разработаны правительственными организациям, таким как Национальный институт стандартов и технологии США (NIST).

[1] Партнерство USAID-NREL: https://www.nrel.gov/usaid-partnership.
[2] Платформа устойчивой энергетики: https://resilient-energy.org.

Продавцы оборудования, консультанты и некоммерческие организации также создали большое количество полезных ресурсов. Настоящий документ содержит выдержки и ссылки на такие руководства, стандарты и наработки.

Однако многие организации все еще прикладывают немалые усилия для создания программы кибербезопасности, которая была бы сбалансирована по всем направлениям, для защиты их активов от атак. Организации могут делать большие вложения в одну область и недостаточные – в другую. Надеемся, что для таких организаций полезным окажется подход с использованием «структурных блоков». **Структурные блоки представляют собой группы соответствующих активностей в рамках сбалансированной программы кибербезопасности** и содержат рекомендации и ресурсы по каждой сфере.

Поскольку структурные блоки подразумевают определенные действия, для них должны быть выделены время и ресурсы персонала, аналогично тому, как время и ресурсы персонала выделяются для деятельности, не связанной с киберпространством (например, бухгалтерия).

Структурные блоки взаимосвязаны, при этом одни структурные блоки поставляют информацию другим и взаимно поддерживают друг друга, поскольку каждый зависит от остальных при построении целостного подхода к кибербезопасности. Структурные блоки и их взаимосвязи изображены на Рисунке 1.

Блок 1: Платформа устойчивой энергетики

Платформа устойчивой энергетики помогает странам и населенным пунктам устранять уязвимости энергосистем путем предоставления стратегических ресурсов и направления поддержки стран для обеспечения планирования и внедрения решений в сфере устойчивой энергетики. Сюда входят рекомендуемые справочные материалы, учебные материалы, данные, инструменты и прямая техническая помощь в планировании надежных, устойчивых и безопасных энергосистем. В конечном счете, такие ресурсы обеспечивают лицам, ответственным за принятие решений, возможность оценивать уязвимость энергетического сектора, находить решения по повышению устойчивости к внешним воздействиям и принимать обоснованные решения по повышению устойчивости энергетического сектора в различных масштабах, включая местный, региональный и национальный уровни. Больше информации о платформе устойчивой энергетики на сайте: https://resilient-energy.org/.

Группы соответствующих активностей, обозначенные структурными блоками кибербезопасности в энергетическом секторе, охватывают несколько задействованных сторон. На рисунках в этом документе блоки, окрашенные сплошной заливкой, являются внутренними для компании, а блоки с градиентом – внешними. Стрелки показывают основные категории информации, передаваемой между структурными блоками. (Стрелки обозначены на Рисунках 2-12 и описаны в сопроводительном тексте.)

Организации на ранних стадиях развития кибербезопасности, скорее всего, получат наибольшую выгоду от применения таких структурных блоков, поскольку они, вероятно, будут усердно работать над тем, как должна выглядеть полная киберпрограмма. Более «зрелые в киберпространстве» организации также могут использовать структурные блоки, чтобы по-новому взглянуть на свою работу и заполнить пробелы в своих существующих киберпрограммах.

Структурные блоки кибербезопасности в энергетическом секторе не являются последним словом в вопросах кибербезопасности для энергетического сектора, поскольку эта сфера быстро развивается с появлением новых технологий электросетей и постоянно меняющимся картинами угроз. USAID и NREL приглашают к обсуждению относительно обновлений для будущих итераций настоящих структурных блоков.

1.1.2 Краткое описание

- **Управление:** Процессы по руководству работами по кибербезопасности в масштабе предприятия и назначению ответственности за такие работы. Управление кибербезопасностью требует понимания и действий со стороны тех, кто находится на самом верхнем уровне предприятия, например, исполнительного директора, главного исполнительного директора (CEO), совета директоров и других.
- **Политика безопасности организации:** Данный структурный блок специализируется на документе высокого уровня, который отображает основные элементы работ предприятия в области кибербезопасности и включает в себя работы по созданию, обновлению и внедрению такого документа.
- **Управление рисками:** Активности по распознаванию и оцениваю риска для кибербезопасности с целью снижения такого риска до уровня, соответствующего бизнес-целям предприятия.
- **Разведка в области киберугроз (CTI):** Инструменты кибератак, злоумышленники, которые могут представлять угрозу, и факторы уязвимости. Предприятия нуждаются в CTI для понимания картины угроз и принятия мер по снижению кибер-рисков.
- **Законы, нормативные акты и стандарты:** Законы и нормативные акты – это обязательные директивы страны места нахождения, которые предприятие должно соблюдать в отношении кибербезопасности. Нормативные акты могут предусматривать соблюдение стандартов, разработанных неправительственными организациями и отражать передовой опыт.
- **Соблюдение норм:** Работы внутри предприятия с целью соответствия законам, нормативным актам и стандартами.
- **Обеспечение:** Процессы, используемые для контроля и повышения кибербезопасности устройств, приложений и сервисов по мере их приобретения и интеграции в работу предприятия, а также работы по управлению рисками в цепочке обеспечения.
- **Технический контроль:** Компоненты оборудования и программного обеспечения, защищающие систему от кибератак. Брандмауэры, системы обнаружения вторжений (IDS), шифрование, механизмы идентификации и аутентификации являются примерами технических средств контроля.
- **Мероприятия по реагированию:** Действия, предпринимаемые предприятием для подготовки к кибератакам. Сюда входит создание планов реагирования, репетиция реагирования перед атакой, постоянный мониторинг для выявления атак и непосредственно реагирование.
- **Обучение основам кибербезопасности:** Меры, предпринимаемые предприятием для ознакомление всех сотрудников (включая нетехнический персонал) с потенциальными киберугрозами и их ролью в предотвращении таких угроз.
- **Подготовка трудовых ресурсов:** Работы большого количества организаций, таких как правительство, промышленность и представители науки, по обеспечению достаточного количества сотрудников, обладающих специальными знаниями и навыками в области кибербезопасности.

1.1.3 Структура

Каждый структурный блок содержит вступление, а также следующие подразделы:

- **Важность.** Почему структурный блок заслуживает внимания.
- **Пересечение с другими структурными блоками.** Основные категории информации, передаваемые между данным структурным блоком и другими. (Включая увеличенные диаграммы элементов из Рисунка1).
- **Процессы и действия.** Основные действия в рамках каждого структурного блока.
- **Важная информация.** Информация, которую организация должна собрать или

сформировать для эффективной работы по каждому структурному блоку.

- **Рекомендованная литература.** Краткий перечень отчетов и статей об основных действиях, освещенных в структурных блоках.

Обратите внимание, приложение в конце документа содержит перечень литературы (использованной в тексте) и дополнительные источники по каждому структурному блоку.

2 Управление

Управление кибербезопасностью энергетического сектора обеспечивает надзор за работами предприятия по кибербезопасности. Посредством управления совет директоров предприятия, главный исполнительный директор (CEO), исполнительное руководство и другие лица, принимающие решения, стремятся сбалансировать распределение ресурсов, риски и бизнес-цели. Руководители должны учитывать риски, связанные с кибератаками, а также необходимость соблюдать государственные и региональные нормативные акты относительно кибербезопасности. Их роль – целостная оценка кибербезопасности с учетом данных о текущих киберуязвимостях, а также влияния ожидаемых обновлений системы, роста диджитализации и расширения системы.

2.1 Важность

Если высшие уровни организации не демонстрируют активных действий в вопросах кибербезопасности, работы предприятия по усилению кибербезопасности не будут особо успешны (если они вообще будут). Один из способов продемонстрировать такие активные действия – выделить ресурсы на оплату рабочего времени персонала, инструментов и, возможно, внешних консультантов. Управление кибербезопасностью должно обеспечивать назначение этих ресурсов туда, где они действительно необходимы – программы кибербезопасности в масштабах организации легко становятся «однобокими», одну область вкладывают слишком много, а в другую – недостаточно. Управление кибербезопасностью включает в себя обеспечение эффективности общей работы по кибербезопасности и ее соответствия потребностям предприятия.

Еще один способ для руководства продемонстрировать свою вовлеченность – убедить сотрудников в том, что каждый из них играет свою роль в обеспечении кибербезопасности. Руководство должно информировать об этом не только словами, но и действиями, подавая пример. Если сотрудники увидят, что руководство игнорирует политики и руководящие принципы кибербезопасности, они быстро поймут, что руководство несерьезно относится к этому вопросу. Своими словами, которые подкреплены действиями, руководство может способствовать развитию культуры кибербезопасности, которая поможет защитить предприятие от будущих кибератак. (Для получения дополнительной информации по данному вопросу см. структурный блок «**Обучения основам кибербезопасности**»).

2.2 Пересечение с другими структурными блоками

Структурный блок «**Управление**» обеспечивает входящие данные (посредством распорядительных актов), которые используются для разработки политики безопасности организации – документа, определяющего работы предприятия по обеспечению кибербезопасности. Лица, принимающие решения в структурном блоке управление, определяют, как будет выглядеть кибербезопасность; политика безопасности организации фиксирует эти решения и представляет их как действенные меры, которые необходимо предпринять.

Управление также обеспечивает соблюдение всех нормативных актов. Резюме требований нормативных актов приведено в структурном блоке «**Соблюдение норм**».

Управление устанавливает цели управления рисками и бизнес-требования, которые определяют объем структурного блока «**Управления рисками**» предприятия.

Структурные блоки «Политика безопасности организации», «Соблюдение норм», и «Управление рисками» больше других взаимодействуют с блоком «Управление»; однако структурный блок «Управление» также полагается на данные, отчеты и другие типы информации остальных структурных блоков, которые могут быть использованы для принятия решений на высоком уровне.

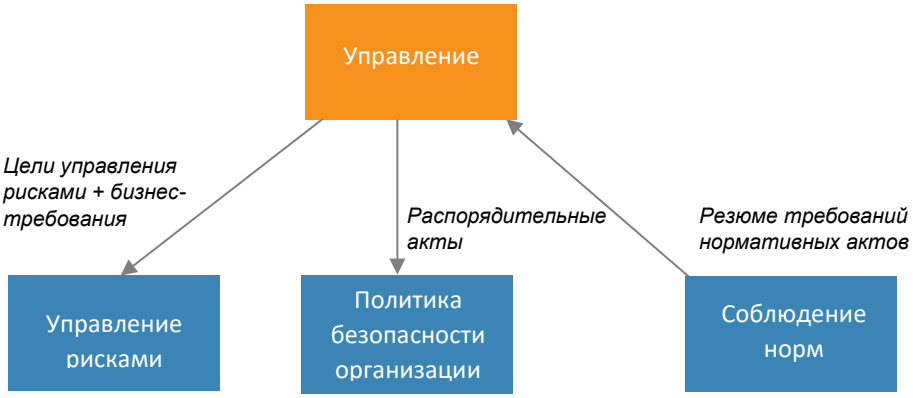


Рисунок 2. Входящая и исходящая информация структурного блока Управление

2.3 Процессы и действия

Структурный блок **«Управление»** объединяет работу других структурных блоков, поэтому процессы и действия данного блока частично совпадают с процессами и действиями остальных структурных блоков данного документа. В Таблице 1 приведено соответствие процессов управления согласно *«Рекомендаций по улучшению кибербезопасности ключевых инфраструктур»* (NIST 2018) и структурных блоков, в которых содержится подробное описание каждого пункта. В контексте рекомендаций NIST данные процессы являются подкатегориями в категории управления.

Таблица 1. Процессы управления NIST

***Рекомендации* NIST**	**Соответствие структурным блокам**
«Политика кибербезопасности организации установлена и доведена до сведения».	Политика безопасности организации
«Роли и обязанности в области кибербезопасности скоординированы и согласованы с внутренними должностными функциями и внешними партнерами».	Управление
«Правовые и нормативные требования в отношении кибербезопасности, включая обязательства в отношении конфиденциальности и гражданских свобод, понятны и соблюдены».	Соблюдение норм
«Процессы управления и управления рисками распространяются на риски кибербезопасности».	Управление рисками

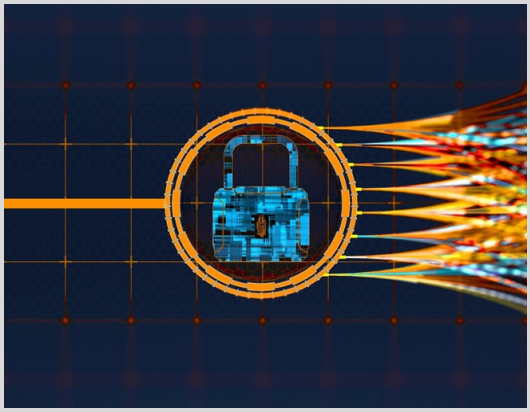
Назначение ролей и обязанностей (вторая строка Таблицы 1) является исключительно сферой деятельности управления кибербезопасностью. Лица, принимающие решения на высоком уровне, должны определить, кто и какие обязанности в рамках политики кибербезопасности будет выполнять, а также создать необходимые структуры отчетности и надзора, необходимые для обеспечения выполнения таких обязанностей.

Осуществление такого надзора требует наличия у лиц, принимающих решения, определенного уровня знаний относительно кибербезопасности.

К сожалению, не все лидеры обладают необходимыми знаниями в этой области (Ротрок, Каплан и Ван дер Оорд, 2017 г.). CEO или совет директоров не обязательно должны быть экспертами в области кибербезопасности, но для принятия обоснованных решений они должна иметь достаточное понимание. Некоторые коммерческие организации предлагают программы обеспечения готовности к кибербезопасности для руководителей и советов директоров (Tyler Cybersecurity, без даты). Некоторые ассоциации также предлагают рекомендации советам директоров (NACD 2020), выдержки из таких ресурсов доступны в Интернете (Бью, без даты). Данные ресурсы предлагают несколько способов, с помощью которых лица, принимающие решения, могут получить необходимые знания для выполнения своих обязанностей в области кибербезопасности.

Для предприятий, которые хотят оценить эффективность своего управления кибербезопасностью, оценивание можно выполнить в NREL. Инструмент оценивания системы кибербезопасности распределенных энергетических ресурсов (DER-CF) охватывает три области, одна из которых – управление (NREL, без даты). См. Подробности в блоке справа.

Блок 2: DER-CF



Оценивание DER-CF охватывает управление, техническое управление и физическую безопасность. DER-CF можно использовать бесплатно в качестве инструмента для самостоятельного оценивания, при этом пользователи могут выполнять оценивание в качестве анонимных посетителей системы (в этом случае предприятию не нужно идентифицировать себя по названию, и никакие данные, связанные с оценкой, не будут сохраняться в системе DER-CF). NREL также может предоставлять директивы предприятиям для оценивания DER-CF; некоторые предприятия ценят участие внешней стороны, которая может облегчить процесс и сообщить результаты руководству предприятия. Больше информации о DER-CF на сайте: **https://dercf.nrel.gov.**

2.4 Важная информация

Для эффективного управления организации должны собрать или сформировать информацию ниже.

- Подробная информация о нормативных требованиях. Данная информация формируется из структурного блока «**Соблюдение норм**».
- Подробная информация о рисках, угрозах и уязвимостях для предприятия. Такую информацию можно почерпнуть из CTI извлечь из структурного блока «**Управление рисками**».
- Бюджетирование. Сколько может предприятие потратить на кибербезопасность? Сколько будет стоить соблюдение норм, и сколько останется для ослабления рисков,

не покрываемых работами по соблюдению норм?

- Внутреннее техническое обеспечение. Какими инструментами и технологиями располагает предприятие для обеспечения работ по кибербезопасности?
- Внутренний кадровый потенциал. Какими знаниями в области кибербезопасности располагает предприятие для осуществления различных необходимых действий в области кибербезопасности? Кроме того, насколько хорошо весь персонал понимает основы ответственного и кибербезопасного использования компьютеров? (см. Структурный блок **«Обучения основам кибербезопасности»**).
- Внешние ресурсы. Где предприятие может получить помощь извне, например рекомендации, консультацию и обучение? К данным ресурсам могут относиться государственные учреждения, представители науки, коммерческие учебные заведения, консультанты или некоммерческие организации.

Рекомендованная литература и дополнительные источники по данному структурному блоку приведены приложении под заголовком «Управление».

3 Политика безопасности организации

Политика безопасности организации – это документ, определяющий объем работ предприятия по обеспечению кибербезопасности. Он выполняет функции хранилища решений и информации, сформированных другими структурными блоками и руководством для принятия будущих решений в области кибербезопасности. Политика безопасности организации должна включать информацию о целях, обязанностях, структуре программы безопасности, соблюдении норм и используемом подходе к управлению рисками.

3.1 Важность

Политика безопасности организации служит справочником для сотрудников и руководителей, выполняющих задачи по внедрению кибербезопасности. Что совет директоров решил в отношении финансирования и приоритетов безопасности? Какие новые правила безопасности были введены правлением и как они влияют на технический контроль и ведение документации? Какой подход к управлению рисками будет использовать организация? Как организация будет реагировать в случая несоблюдения сотрудником обязательных политик безопасности?

Политика безопасности организации служит основным документом для решения многих подобных вопросов. Она выражает вовлечение руководства в вопросы безопасности, а также определяет, что компания будет делать для достижения своих целей в области безопасности.

3.2 Пересечение с другими структурными блоками

Поскольку политика безопасности организации играет основную роль в фиксировании и доведении до сведения информации о работах по безопасности в масштабах предприятия, она затрагивает многие другие структурные блоки. Структурный блок «**Управление»** вырабатывает решения высокого уровня, воздействующие на другие структурные блоки. Структурный блок «**Соблюдение норм»** определяет, что предприятие должно делать для соответствия утвержденным правительством стандартам безопасности. Политика безопасности организации фиксирует оба эти блока информации.

Подход предприятия к управлению рисками (рекомендации, которые оно будет использовать) установлен в политике безопасности организации и использует структурный блок «**Управление рисками»** для разработки стратегии по управлению рисками. Цели, определенные в политике безопасности организации, переходят на структурные блоки **«Обеспечение»**, **«Технический контроль»**, **«Мероприятия по реагированию»**, и **«Обучение основам кибербезопасноти»**.

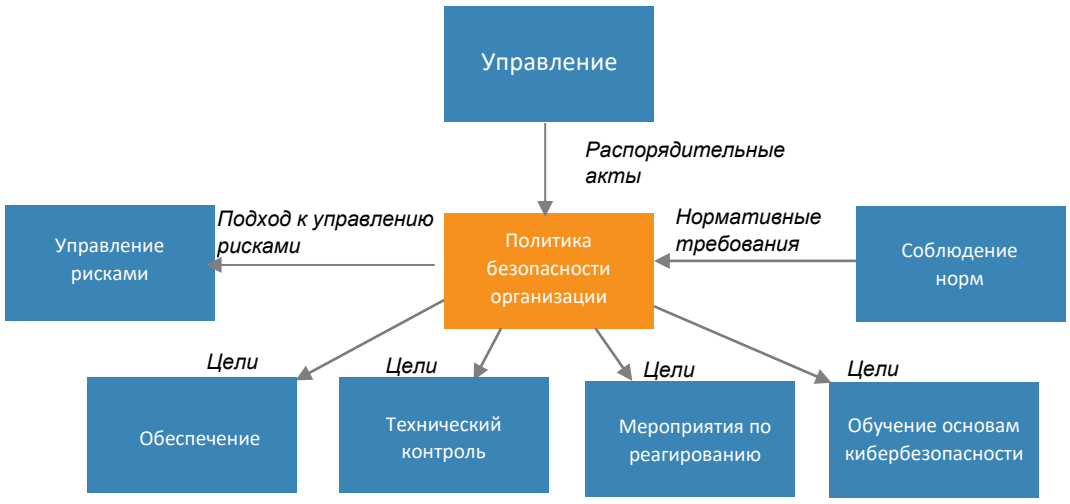


Рисунок 3. Входящая и исходящая информация структурного блока Политика безопасности организации

3.3 Процессы и действия

Разработка политики безопасности организации требует вовлеченности многих различных представителей внутри организации. У политики должен быть «собственник» – человек с достаточными полномочиями для вовлечения нужных людей с момента запуска процесса и до его финальной реализации. Собственник также несет ответственность за контроль качества и полноту работы (Ки, 2001). Назначение собственника политики – хороший первый шаг в разработке политики безопасности организации.

Собственник политики должен будет определить задействованные стороны, в том числе технический персонал, лиц, принимающих решения, и тех, кто будет нести ответственность за соблюдение политики. В идеале, собственник политики должен быть руководителем группы, которой поручено разработать политику. Все должны согласовать политику на этапе рассмотрения и подписать ее, прежде чем она может быть завершена.

Лица, принимающие решения по предприятию – совет директоров, CEO, исполнительный директор и т.д. – должны определить бизнес-цели, которые будет поддерживать политика безопасности, и назначить ресурсы для ее разработки и внедрения. Бизнес-цели должны определять политику безопасности, а не наоборот (Харрис и Мэйми, 2016, 88).

Предприятию необходимо будет провести инвентаризацию активов, при этом особое внимание будет уделено наиболее критичным аспектам. Необходимо проанализировать угрозы и уязвимости и определить их приоритетность. Также можно определить меры по смягчению таких угроз, затраты и степень снижения риска.

Политике определяет роли и обязанности всех, задействованных в программе безопасности предприятия. Руководству предприятия необходимо будет назначить (или, по крайней мере, утвердить) данные обязанности. Задачи обучения основам кибербезопасности должны быть указаны на равне с последствиями для сотрудников, которые либо пренебрегают участием в обучении, либо не соблюдают стандарты поведения в отношении кибербезопасности, установленные организации (см. Структурный блок **«Обучение основам кибербезопасности»** для получения дополнительной информации).

Политика может быть структурирована как один документ или как иерархия, с одной

основной политикой и множеством политик по конкретным аспектам (Харрис и Мэйми, 2016, 88). Институт SANS бесплатно предлагает шаблоны политик по конкретным аспектам («Шаблоны политик безопасности», без даты); к данным шаблонам относятся:

- Приемлемая политика шифрования
- Политика при нарушении безопасности данных
- Политика в отношении использования Интернет
- Политика в отношении удаленного доступа
- Политика оценки угроз
- Политика осведомленности о информационно-психологических атаках
- Политика в отношении виртуальной выделенной сети.

Когда политика составлена, она должна быть рассмотрена и подписана всеми вовлеченными сторонами. Необходимо установить периодичность проверок и пересмотра, чтобы политика соответствовала изменениям бизнес-целей, угрозам для организации, новым правилам и другим важным изменениям, влияющим на безопасность.

3.4 Важная информация

При создании или обновлении политики безопасности организации следует собрать следующую информацию, поскольку эти составляющие помогут правильно сформировать политику.

- Список вовлеченных сторон, которые должны внести свой вклад в политику, и список тех, кто должен подписать окончательную версию политики
- Инвентаризация активов с приоритетом критичности
- Данные о прошлых кибератаках, включая вызванные ошибками сотрудников (например, открытием зараженного вложения электронной почты). Это предоставит информацию, необходимую для постановки задач структурного блока **«Обучение основам кибербезопасности»**.
- Риски и уязвимости, которые могут оказать влияние на предприятие.

Также предприятию нужно собрать следующие данные и внедрить их в политику безопасности организации:

- Бизнес-цели (определенные лицами, принимающими решения по предприятию)
- Законы, нормативные акты, и стандартны, применимые к предприятию, в том числе те, которые ориентированы на безопасность, кибербезопасность, конфиденциальность и требуемое раскрытие информации в случае успешной кибератаки.

Рекомендованная литература и дополнительные источники по данному структурному блоку приведены приложении под заголовком «Политика безопасности организации».

4 Управление рисками

Управление рисками это практика организации, направленная на снижение рисков в рамках всей организации. Потребности и миссия организации определяют приоритетность, в которой рассматриваются риски. Риск нельзя полностью исключить, всегда будет некоторый уровень остаточного риска, даже после его устранения. Определить, какой риск готова принять на себя организация,– задача, с которой сталкивается каждая организация.

4.1 Важность

Управление рисками кибербезопасности имеет решающее значение для работы энергетической системы и всего, что с ней связано. Риски, с которыми сталкивается организация, определяют ключевые области, требующие особого внимания, во избежание потенциальных угроз. Осведомленность о рисках поможет организации определить, какой риск она готова принять. После того, как будут определены риски и их приоритетность, может быть составлен план действий по снижению уязвимости. (Определения «риска» и других терминов блока «Управления рисками» см. в Блоке 3)

Управление рисками – это длительный и трудоемкий процесс. Стратегия управления рисками кибербезопасности, направленная на предотвращение, оценку и снижение рисков, поможет обеспечить структурированность и целостность организации.

4.2 Пересечение с другими структурными блоками

Решения относительно целей риска являются бизнес-решениями и, следовательно, принимаются на самом высоком уровне предприятия (советом директоров, CEO, исполнительным директором и т. д.). Целью предприятия является повышение надежности обслуживания? Уменьшение количества инцидентов, связанных с вредоносным ПО? Снижение стоимости?

Подобные решения являются составляющими структурного блока **«Управление»** и пересекаются со структурным блоком «**Управление рисками»** в аспектах целей рисков и бизнес-требований.

Управление рисками кибербезопасности затрагивает каждый аспект организации и зависит от правильных политик и процедур. Политика безопасности организации отображает подход предприятия в управлении кибер-рисками. Сюда относятся четко обозначенные роли и зоны ответственности, обеспечивающие подотчетность за риски в рамках всей организации.

Управление рисками должно учитывать меняющуюся картину угроз, отображаемую CTI. Большинство предприятий зависят от внешних источников такой информации, которая включает данные о возникающих угрозах (например, новых хакерских группах), новых уязвимостях (например, недавно обнаруженный недостаток безопасности операционной системы) и новых инструментах кибератак (например, новое вредоносное ПО).

Внедрение CTI в управление рисками позволяет предприятию выявить возможные угрозы и уязвимости, а также разработать план по их устранению. План должен включать приоритетность угроз в зависимости от определенного организацией уровня риска. Чем выше риск для критически важных операций, тем выше эта угроза должна стоять в списке приоритетов.

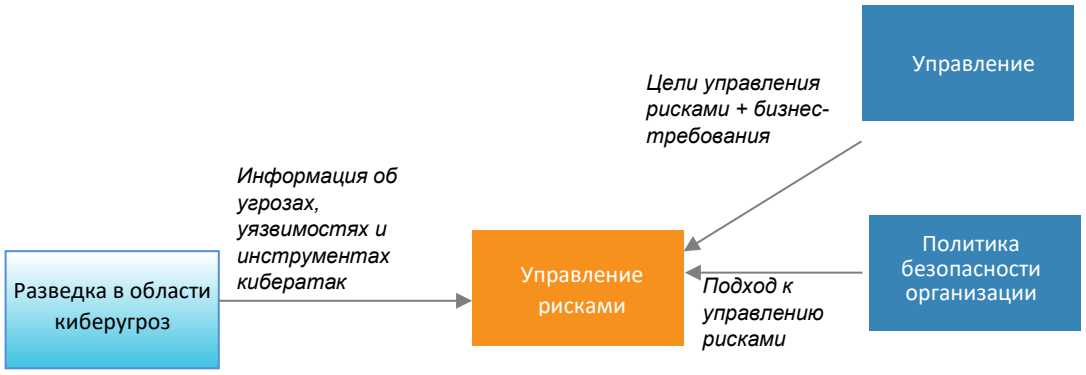


Рисунок 4. Входящая и исходящая информация структурного блока Управление рисками

4.3 Процессы и действия

У организаций есть четыре варианта управления рисками:

- *Избежание риска.* Если приложение или поведение сотрудников представляет собой риск, просто запретите его. Например, если сотрудники, проверяя свою личную электронную почту на рабочих компьютерах, разрешают проникновение вредоносного ПО в сеть, не разрешайте использование личной электронной почты на рабочих компьютерах.
- *Принятие риска.* Узнайте, можно ли «пережить» риск. Принимая это решение, организациям необходимо тщательно рассмотреть потенциальный вред, который представляет риск, и вероятность того, что этот риск будет иметь место.
- *Устранение риска.* Установите меры безопасности, снижающие риск. Например, размещение брандмауэра между внутренней сетью и общедоступным Интернетом снижает риск сетевой атаки. Обратите внимание, такие меры не устраняют риск полностью, цель состоит в том, чтобы снизить риск до приемлемого уровня. Риск, остающийся после усиления мер безопасности, называется остаточным риском.
- *Передача риска.* Возложите ответственность за риск на другую сторону. Классический пример – покупка страховки, которая перекладывает риски на страховую компанию.

Решения о том, как справляться с различными типами риска и другие, связанные с риском, вопросы лучше всего отразить в *стратегии управления рисками*. Это позволит определить правильное применение средств контроля кибербезопасности в средах информационных технологий (ИТ) и систем управления производственными процессами (ICS). Стратегия должна включать периодическое оценивание уязвимости и рисков, с целью определить присутствующие риски присутствуют, затем риски фиксируют в документе, который называется *реестром рисков*. Часть стратегии управления рисками заключается в выборе показателей риска для ранжирования или определения приоритетности рисков. Создание стратегии управления рисками требует усилий, но ее результат - налаженные бизнес-процессы и процессы принятия решений.

Существует несколько различных моделей методик управления рисками. Приведенные ниже элементы адаптированы и резюмированы из работы «*Процесс управления рисками подсектора электроэнергетики»* (Министерство энергетики США, 2012 г.).
Правильно составленная стратегия управления рисками кибербезопасности должна включать, помимо прочего, следующее:

- Определение ключевых задействованных сторон, а также их роли и обязанности. В «Процессе управление рисками» Министерства энергетики США перечислены многие возможные задействованные стороны, включая руководителей высшего звена, собственников бизнес-процессов, руководителей информационных служб или служб безопасности, а также владельцев информационных систем. Однако не все из них, вероятно, имеют возможность и/или заинтересованы в участии в управлении рисками.
- Определение методик оценивания и приоритезации рисков и уязвимостей кибербезопасности.
- Определение и приоритезация рисков организации на основании миссии и того, что является наиболее важным, вероятности реализации риска и серьезности его воздействия в случае реализации. Это требует понимания систем и активов, их взаимосвязей, параметров связи и поведения.
- Определение уровня терпимости организации к риску. Какой риск организация готова/способна принять на себя? Терпимость к риску организации должна учитывать шаги, которые потребуются организации для восстановления в случае инцидента.
- Разработка бизнес-процессов с учетом рисков, принимая во внимание угрозы и риски кибербезопасности, а также рекомендаций относительно мер по их предотвращению.
- Определение и расстановка приоритетов IT и ICS инструментов, необходимых для поддержки бизнес-процессов с учетом рисков.
- Внедрение процесса регулярной переоценки состояния кибербезопасности системы на основе новой информации об угрозах, уязвимостях или системных изменениях.

Более детализированный подход и описание процессов управления рисками приведен в работе «*Процесс управления рисками подсектора электроэнергетики»* (Министерство энергетики США, 2012 г.).

4.4 Важная информация

При разработке стратегии управления рисками кибербезопасности компания должна собрать следующую информацию:

- Список вовлеченных сторон организации
- Стратегия управления рисками по всей организации. Другими словами, любые существующие стратегии управления рисками, не относящиеся к кибербезопасности. Стратегию управления рисками кибербезопасности необходимо согласовать с этими другими стратегиями.
- Миссия организации
- Стратегические цели и задачи организации
- Текущие бизнес-процессы в отношении систем IT и ICS
- Инвентаризация активов с приоритетом в соответствии с важностью для миссии
- Роли обязанности применительно к кибербезопасности.

Блок 3: Терминология управления рисками

- **Угрозы.** Все, что может повредить, разрушить или нарушить энергетический сектор. Угрозы могут быть естественными, технологическими или антропогенными. Угрозы обычно находятся вне контроля проектировщиков и операторов энергосистем. Они могут включать лесные пожары, ураганы, штормовые нагоны, кибератаки и многое другое.
- **Воздействие.** Степень, в которой угроза влияет на инфраструктуру, системы или процессы энергетического сектора (например, торнадо вызывает повреждение линий электропередач ветром).
- **Уязвимости.** Слабые места в инфраструктуре, процессах и системах или степень уязвимости к различным угрозам. Могут быть приняты различные меры для снижения уязвимости или повышения способности адаптироваться к угрозам в энергетическом секторе.
- **Риск.** Возможность утраты, повреждения или разрушения ключевых ресурсов или активов энергосистемы в результате воздействия угрозы. Риск иногда оценивается как производная вероятности угрозы и уязвимости системы.

Обсуждение этих терминов и ресурсы для количественной оценки и ранжирования рисков можно найти на странице: **https://resilient-energy.org/guidebook**

Рекомендованная литература и дополнительные источники по данному структурному блоку приведены приложении под заголовком «Управление рисками».

5 Разведка в области киберугроз

Разведка в области киберугроз (CTI) Разведка в области киберугроз (CTI) – это информация об угрозах, уязвимостях и инструментах кибератак, которые организация должна знать, чтобы обеспечить для себя лучшую защиту. Данные CTI собирают государственные учреждения, некоммерческие организации, ученые и коммерческие организации. Эти организации публикуют уведомления и предупреждения по мере развития угроз, обнаружения новых уязвимостей и выявления новых инструментов атаки. Данные CTI иногда предоставляются бесплатно, а иногда требуют платной подписки. Центры обмена информацией и анализа (ISAC) предоставляют CTI для конкретных отраслей (например, электроэнергетики, авиации и финансовых услуг).

5.1 Важность

Располагая актуальными данными CTI, организация может оптимизировать свои работы по кибербезопасности и лучше распределить свои затраты на оценивание и устранение уязвимостей, которые могут быть целью конкретных киберугроз. Когда, например, растет число программ-вымогателей, вложения в обучение персонала основам кибербезопасности снизят уязвимость недостаточно подготовленных сотрудников (которые могут, например, открыть вложение электронной почты, зараженное вредоносным ПО). Если количество сетевых атак увеличивается, рассмотрите усиление изоляции сети и обнаружения вторжений.

Понимание того, кто и как может атаковать и какие уязвимости они могут использовать, обеспечивает лучшую готовность организации к защите.

5.2 Пересечение с другими структурными блоками

Структурный блок **«Разведка в области киберугроз»** пересекается с информацией структурного блока «**Управление рисками»** применительно к возникающим угрозам (например, новые хакерские группы), новым уязвимости (например, недавно обнаруженный недостаток безопасности операционной системы) и новым инструментам кибератак (например, новое вредоносное ПО). Такая информация дает управлению рисками более полное представление о рисках, с которыми сталкивается организация, и используется для определения приоритетов ресурсов безопасности.

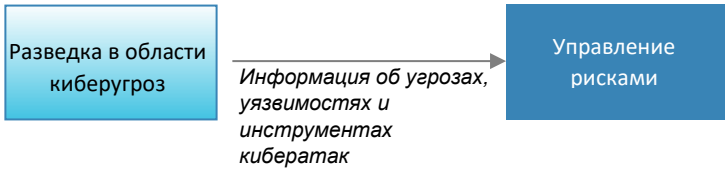


Рисунок 5. Входящая и исходящая информация структурного блока Разведка в области киберугроз

5.3 Процессы и действия

Данные CTI генерируют некоммерческие организации, государственные учреждения и коммерческие организацие, которые специализируются на мониторинге и анализе постоянно меняющейся картины киберугроз. CTI используется многими типами организаций (включая энергетические компании); однако, прежде чем организация начнет мониторинг источников CTI, ей следует провести тщательную инвентаризацию своих активов – используемых систем, устройств, приложений и программного обеспечения. Такие активы должны быть ранжированы по критичности. Список активов с указанием приоритетности позволяет

организации сосредоточиться на наиболее актуальных предупреждениях и уведомлениях. Если предупреждение или уведомление касается угрозы для типа устройства, которого нет в организации, его можно проигнорировать. В качестве альтернативы, если у организации есть устройство, но оно используется в условиях с низкой или средней критичностью, срочность ответа на предупреждение или уведомление будет ниже. Инвентаризация активов, упорядоченная по степени важности, позволяет определить приоритеты реагирования.

Затем организация должна решить, какие из ресурсов CTI она будет отслеживать. Их достаточно много и организации следует ознакомиться с ресурсами CTI, чтобы определить, какие из них соответствуют ее потребностям и бюджету.

Некоторые источники CTI предназначены для определенных промышленных систем управления или электроэнергетики, тогда как другие носят более общий характер. Некоторые взимают плату за предоставляемую информацию, а другие предоставляются бесплатно. Консультанты по безопасности составили списки источников CTI вместе с руководством по их оценке (Метивье, 2016). В списке ниже приведены примеры источников CTI от правительственных, некоммерческих и коммерческих организаций. Примечание: список содержит примеры и не является поддержкой какого-либо конкретного источника CTI.

- **Spamhaus Project** (www.spamhaus.org)
  - Международная некоммерческая организация со штаб-квартирой в Швейцарии.
  - CTI общего характера
  - Бесплатная общественная услуга (с определенными ограничениями).
- **SANS Internet Storm Center** (isc.sans.edu)
  - Частная компания (SANS Institute)
  - CTI общего характера
  - Бесплатная общественная услуга.
- **ICS-CERT** (www.us-cert.gov/ics)
  - Правительственная программа США
  - CTI предназначенные для ICS
  - Бесплатная общественная услуга.
- **RSA** (www.rsa.com)
  - Частная компания
  - Для определенных сфер, имеет автоматизированную сегментацию
  - Платная подписка.
- **National Council of ISACS** (www.nationalisacs.org)
  - Координатор 20 отдельных ISACS
  - Каждый ISAC посвящен определенному секторы (например, ISAC для сектора электричества)
  - Некоторые ISACS имеют бесплатный доступ, некоторые – открыты только для подписчиков.

Наибольшее внимание следует уделять угрозам, направленным на самые важные системы и данные, следовательно, приоритезация этих критически важных объектов поможет обосновать выбор источников CTI.

Затем организациям необходимо решить, кто будет отслеживать источники CTI и какие ответные действия будут предприняты. Нет смысла собирать CTI, если ни на кого не возложена ответственность за отслеживание предупреждений или уведомлений. В бюджете необходимо выделить время, необходимое для отслеживания предупреждений и уведомлений CTI и реагирования на них. Высшее руководство должно проинструктировать

персонал всех отделов, чтобы они были готовы оказывать сотрудничество в работах по реагированию на предупреждения и уведомления (например, по устранению недавно обнаруженной уязвимости).

После этого организация может начать мониторинг источников CTI. Отдельные предупреждения и уведомления могут потребовать принятия мер (например, устранения недавно обнаруженной уязвимости), в то время как долгосрочные тенденции в CTI становятся исходными данными для структурного блока **«Управления рисками».**

5.4 Важная информация

Организациям, планирующим отслеживание CTI, следует ознакомиться с источниками, которые больше всего соответствуют их потребностям. Сбор следующей информации поможет им сделать выбор из множества доступных источников:

- Инвентаризация активов организации, упорядоченная по степени важности
- Список источников CTI, упорядоченный по степени применимости к важным активам компании
- Процессы и планы ответа на CTI.

Рекомендованная литература и дополнительные источники по данному структурному блоку приведены приложении под заголовком «Разведка в области киберугроз».

6 Законы, нормативные акты и стандарты

Законы и нормативные акты вводятся в действие правительством с целью определения стандартов поведения физических лиц, корпораций или других организаций. Законы принимаются законодательными или другими уполномоченными органами. Правительственные органы вводят в действие нормативные акты, определяющие порядок применения закона. Законы и нормативные акты, применимые к электроэнергетическим компаниям, предназначены для повышения надежности, безопасности, доступности и защищенности сетей «Рамочные принципы оценки киберпространства для регуляторов в районе Черного моря», 2017, 5).

Нормативные акты иногда включают стандарты – передовые методы, собранные и проверенные надежными организациями. Например, Международная организация по стандартизации (ISO) и Международная электротехническая комиссия (IEC) совместно опубликовали серию стандартов ISO/IEC 27000 относительно информационной безопасности. Когда стандарты включены в нормативные акты, их соблюдение естественным образом включает соблюдение стандартов. Организации (включая энергетические компании) могут принять решение соблюдать определенные стандарты, даже если они не обязаны этого делать по законам. Это может обеспечить внутренним задействованным сторонам (например, высшему руководству) уверенность в том, что организация применяет разумные меры безопасности.

Блок 4: Три типа стандартов
В сфере кибербезопасности слово «стандарт» имеет много значений

- *Стандартны лучших практик,* как ISO/IEC27000 (описанное слева).
- *Технические стандарты,* которые определяют принципы работы и взаимодействия технологий, например, Стандарт 802.11 Института инженеров электротехники и электроники, определяющий беспроводные протоколы, используемые в сетях Wi-Fi («IEEE 802.11» 2020).
- *Стандарты,* разрабатываемые организацией и соблюдаемые внутри нее, например, как часто сотрудникам нужно менять свои пароли.

Все определения верны, и предполагаемое значение устанавливается из контекста. (Харрис и Мэйми, 2016).

Государственные учреждения в разных странах по-разному подходят к законам и нормативным актам. Законы разных стран могут быть структурированы таким образом, что модели регулирования будут существенно отличаться. Кроме того, учреждения, которым поручено разрабатывать и обеспечивать соблюдение нормативных требований в энергетическом секторе, также различаются, и это может повлиять на применение нормативных требований. В Соединенных Штатах Североамериканская корпорация энергетической надежности устанавливает стандарты надежности, включая кибербезопасность. В Великобритании Управление по рынкам газа и электроэнергии устанавливает правила, к которым относится и кибербезопасность. В Индии эту функцию выполняет Центральная комиссия по регулированию электроэнергетики. Оптимальное регулирование кибербезопасность – непростая задача, различие приоритетов стран требует внедрения различных стандартов.

6.1 Важность

Законы и нормативные акты стимулируют энергетические компании к принятию эффективных мер кибербезопасности (Рагацци и другие, 2020). Такая мотивация может включать выгоды за усиления кибербезопасности или последствия за невыполнение данного

требования. Правильно структурированное нормативные акты уравновешивает выгоду от соблюдения норм в области кибербезопасности и издержки предприятия. Однако разработка «правильно структурированных» нормативных актов может быть непростой задачей, а последствия их неправильного использования могут быть губительными. Плохо структурированные нормативные акты могут вынудить энергетические компании тратить свои ресурсы на их соблюдение и при этом получать небольшую реальную пользу для кибербезопасности. Это может привести к тому, что электрическая сеть станет даже менее безопасной, чем в случае отсутствия каких-либо нормативных актов. Другими словами, организация могла бы достичь большей кибербезопасности, если бы она инвестировала свои ресурсы по своему усмотрению, а не тратила средства на соблюдение плохо структурированных правил.

Признанные на международном уровне стандарты имеют высокую ценность, поскольку отображенный в них передовой опыт проходит тщательную проверку. Они также предоставляют «общий язык» для профессионалов в области безопасности.

6.2 Пересечение с другими структурными блоками

Законы и нормативные акты внедряются правительством для определения требуемого поведения. Стандарты могут внедряться различными организациями (включая международные органы по стандартизации) и определять рекомендуемое поведение. Работы по соблюдению норм внутри предприятия направлены на то, чтобы интерпретировать и ввести в действие такое поведение, а также задокументировать соблюдение предприятием правил и стандартов.

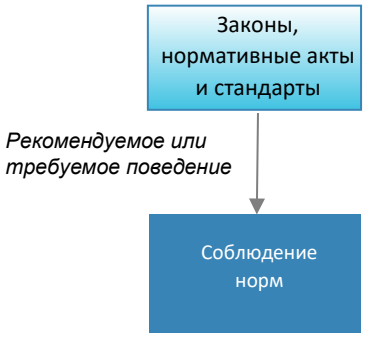


Рисунок 6. Входящая и исходящая информация структурного блока Законы, нормативные акты и стандарты

6.3 Процессы и действия

Пункты, приведенные ниже, были адаптированы и резюмированы из публикации *«Оценка обоснованности инвестиций в кибербезопасность. Методические указания для органов регулирования энергетики»* (Рагацци и другие, 2020), которая содержит расширенное описание всех данных аспектов.

Государственные органы, стремящиеся внедрить или пересмотреть структуру регулирования кибербезопасности, должны сначала решить, какой тип регулирования будет наиболее эффективным для их целей.

Регулирование по показателям эффективности

При регулировании по показателям эффективности регулирующие органы определяют цели безопасности и индикаторы (метрики), которые должны использоваться для подтверждения

соблюдения норм (посредством аудитов или инспекций). Предприятие определяет, как достичь этих целей.

Процесс создания регулирования по показателям эффективности начинается с определения стратегии кибербезопасности. Затем следует определение целей, соответствующих стратегии. Далее определяются индикаторы целей и экономические стимулы их для достижения. Регулирующие органы проводят аудит или инспекцию на предмет соблюдения норм. Со временем регулирующий орган должен обновить структуру на основе отзывов энергетических компаний или собственных наблюдений касательно эффективности структуры.

Регулирование по стоимости обслуживания

При регулирования по стоимости обслуживания регулирующие органы определяют цели и способы их достижения. Регулирующий орган также определяет и оценивает затраты на меры безопасности. Такое регулирование также называют «затраты плюс».

Процесс установления регулирования по стоимости обслуживания начинается с определения стратегии кибербезопасности – по аналогии с регулированием по показателям эффективности. Однако второй шаг переходит к определению контрмер, которые будут использоваться в рамках стратегии. Затем регулирующий орган определяет расходы, связанные с такими контрмерами. Процедуры подотчетности разрабатываются регулирующим органом, который затем проверяет соблюдение предприятием предписанных контрмер. Со временем регулирующий орган должен обновить структуру на основе отзывов энергетических компаний или своих собственных наблюдений касательно эффективности структуры.

Экономическая эффективность

Ключевым фактором любой модели является способность сопоставить стоимость определенного средства контроля безопасности (также называемого контрмерой) с выгодой, обеспечиваемой такой контрмерой. В этом отношении полезно рассмотреть альтернативные сценарии, в которых в предприятии действуют или не действуют регулирования, а затем рассчитать различные затраты как при нормальных условиях работы, так и при кибератаках. Затем для каждого из данных условий взвешиваются затраты на выполнение регулирований и предотвращенные затраты на кибератаки. Данное упражнение детально изложено в публикации *«Оценка обоснованности инвестиций в кибербезопасность. Методические указания для органов регулирования энергетики»* (Рагацци и другие, 2020).

Экономически эффективное регулирование разрабатывается регулирующим органом совместно с регулируемыми лицами – энергетическими компаниями. Регулирование не должно быть односторонним или состязательным.

Регулирование должно исходить из предположения, что все стороны преследуют одну и ту же цель – повышение безопасности – и уникального ценного понимания того, как лучше всего достичь этой цели.

Независимо от типа используемой модели, государственные органы могут выбрать включение одного или нескольких международных стандартов передовой практики в свои нормативные акты. Это является отправной точкой как для регулирующих органов, так и для энергетических компаний, потому что для каждого широко признанного стандарта имеется руководство по его эффективному внедрению.

6.4 Важная информация

Органы, стремящиеся внедрить или пересмотреть структуру регулирования кибербезопасности, должны собрать такую информацию:

- Список текущего действующего регулирования (в отношении кибербезопасности и остального)
- Информация об энергетических компаниях, на которые будут распространяться новые или измененные правила. Такая информация должна включать подробную информацию о самой системе (размер и тип выработки энергии, нагрузки и т. д.), и экономическую информацию о текущей структуре возмещения затрат предприятия, киберподготовленность оборудования и персонала предприятия
- Точки соприкосновения внутри предприятия или энергетической компании, которые будут регулироваться
- Угрозы, которые могут воздействовать на функционирование предприятия (как в области кибербезопасности, так и другие), и вероятные экономические последствия таких угроз.

Рекомендованная литература и дополнительные источники по данному структурному блоку приведены приложении под заголовком «Законы, нормативные акты и стандарты».

7 Соблюдение норм

Соблюдение норм относится к ответственности и работам внутри предприятия по соблюдению законов, постановлений и стандартов, которые могут быть наложены на национальном или региональном уровне. Соблюдение норм может потребовать применения технических средств контроля (например, брандмауэров), административных средств контроля (таких как обучение персонала) или физических средств контроля (таких как замки и ограждения).

7.1 Важность

Директивы правительства и регулирующих органов определяют конкретные модели поведения в области кибербезопасности. Часто такое поведение обеспечивается посредством аудитов или инспекций регулирующего органа или посредством самостоятельного документирования со стороны предприятия. Хотя аудит может показаться обременительным, он также дает возможность получить обратную связь от внешней стороны – аудитора – относительно мер безопасности и механизмов подотчетности. Такая обратная связь может послужить свежим взглядом, который поможет предприятию повысить уровень безопасности.

Несоблюдение норм наказуемо. То, как определены такие штрафы, а также серьезности нарушения влияют на масштабы финансовых последствий (Уоркентин 2019). Но последствия могут быть не только финансовым – несоблюдения норм также может повлиять на репутацию компании и доверие клиентов (Уэст, 2019).

Нормативные акты могут побудить лиц, принимающих решения, выделить ресурсы на кибербезопасность, которые в противном случае не могли бы появиться. Некоторые менеджеры по информационным технологиям заметили, что без нормативных актов они могут не получить от своего начальства финансирование на кибербезопасность. Если законы и нормативные акты хорошо структурированы, они могут дать толчок программе кибербезопасности предприятия, которая со временем может стать более зрелой. (Разъяснения относительно «хорошо структурированных» и «плохо структурированных» нормативных актов приведены в структурном блоке **«Законы, нормативные акты и стандарты»**).

7.2 Пересечение с другими структурными блоками

Структурный блок «Соблюдение норм» по предприятию определяет все применимые законы, нормативные акты и стандарты и разъясняет, как рекомендуемые или требуемые правила поведения применяются по предприятию. Структурный блок «Соблюдение норм» предоставляет важную информацию относительно нормативных требований для структурного блока «Управление». Это позволяет руководству предприятия принимать обоснованные решения относительно распределения ресурсов безопасности. Для блока «Политика безопасности организации» предоставлены более подробные нормативные требования, так что работы по соблюдению внешних норм и внутренние работы по управлению рисками могут быть скоординированы в рамках всей организации.

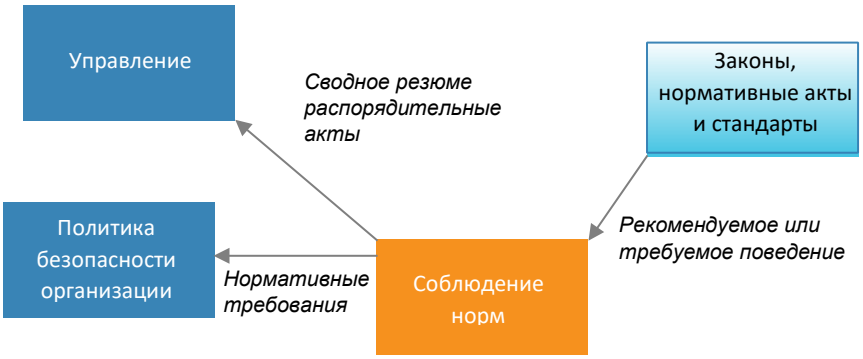


Рисунок 7. Входящая и исходящая информация структурного блока Соблюдение норм

7.3 Процессы и действия

Формирование политик организаций относительно поведения и стандартов кибербезопасности, определенных в нормативных актах, требует тщательного рассмотрения. Хороший первый шаг – найти кого-то, кто имеет опыт (или, по крайней мере, заинтересованность) в нормативных актах и их соблюдении, и кто может взять на себя ответственность за соблюдение норм на предприятии. Такой человек становится *ответственным за соблюдение норм* по предприятию.

Ответственный за соблюдение норм руководит группой других сотрудников (и, возможно, внешними консультантами) при выполнении следующих работ:

- Поиск законов, нормативных актов и стандартов, которые распространяют свое действие на предприятие и относятся к кибербезопасности, конфиденциальности, раскрытию информации о киберинцидентах и другим подобным вопросам
- Если нормативные акты имеют многоуровневую структуру – например, если на более крупных генерирующих предприятиях лежит более тяжелая нагрузка регулирующих органов, – требуется определить, какой уровень соблюдения норм применим к предприятию и какие задачи по соблюдению норм необходимо выполнить
- Поиск любых источников, которые могут помочь при разработке политик и процедур по соблюдению норм
- Взаимодействие с органами власти и перевод требований в рамках всей организации
- Разработка процесса сбора информации относительно процедур соблюдения норм и документирование инцидентов, соответствующих и не соответствующих действующим правилам
- Разработка механизма аудита и пересмотра соблюдения норм внутри предприятия
- Разработка механизма отчетности для подачи периодических статусов по соблюдению норм.

7.4 Важная информация

При внедрении системы соблюдения норм предприятию необходимо собрать следующую информацию:

- Распорядительные правительственные акты
- Стандарты и директивы, утвержденные регулирующими органами
- Стандарты, которые предприятию следует выбрать для соблюдения
- Региональные/национальные/местные законы и требования

- Список критичных систем по предприятию, а также устройств и приложений, работающих в этих системах. Такой список понадобится ответственному за соблюдение норм, если в нормативных актах предусмотрены специальные меры для определенных типов систем.

Рекомендованная литература и дополнительные источники по данному структурному блоку приведены приложении под заголовком «Соблюдение норм».

8 Обеспечение

Обеспечение – это процесс, посредством которого предприятие приобретает устройства, приложения или службы, которые будут внедрены в систему. Хотя иногда это называют просто закупкой, обеспечение на самом деле представляет собой многоступенчатый процесс, который включает в себя определение требований, оценку вариантов покупки, согласование контрактов, закупку и получение устройств или приложений (Харрис и Мэйми, 2016) или активацию услуги.

8.1 Важность

Общая безопасность предприятия в значительной степени зависит от безопасности отдельных устройств, приложений или служб внутри предприятия. Технические средства контроля могут несколько компенсировать пробелы в безопасности данных продуктов, но полученная в результате система никогда не будет столь же надежной, как система, построенная с нуля с использованием безопасных компонентов. Устройства, приложения или службы могут быть небезопасными из-за ошибок, допущенных при их разработке или реализации функций безопасности или же они могут быть сделаны небезопасными намеренно, чтобы злоумышленники могли получить доступ к системам после их установки.

Таким образом, обеспечение играет важную роль в обеспечении кибербезопасности. По крайней мере, тщательный подход к процессу обеспечения дает энергетическим компаниям возможность узнать о состоянии безопасности различных продуктов. В лучшем случае, предприятие может использовать обеспечение с целью выбора безопасных продуктов, одновременно сообщая поставщикам, что кибербезопасность является ключевым аспектом при выборе продукта. Если поставщики узнают, что кибербезопасность является важным фактором при принятии решения о покупке, они, вероятно, вложат больше ресурсов, чтобы сделать будущие продукты более безопасными.

Для энергетических компаний кибербезопасность должна быть основным фактором на всех стадиях обеспечения.

8.2 Пересечение с другими блоками

Политика безопасности организации должна содержать руководства по внедрению кибербезопавсности в процесс обеспечения. Сюда могут входить нормативные требования относительно обеспечения, вытекающие из структурного блока **«Соблюдение норм»**. Сотрудники предприятия, которые проводят анализ требований к покупкам новых устройств и приложений, отправляют запросы на предложения, рассматривают предложения поставщиков, оформляют на покупку, и отвечают за их получение, должны соблюдать данные руководства предприятия.

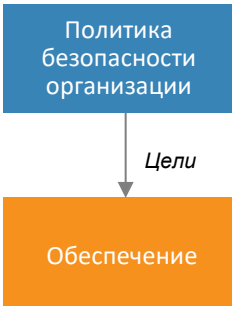


Рисунок 8. Входящая и исходящая информация структурного блока Обеспечение

8.3 Процессы и действия

В последние годы большое внимание уделяется вопросам безопасности, связанным с обеспечением и цепочками поставок. Многие страны, включая Россию, Индию, Китай и США, работают над улучшением кибербезопасности цепочки поставок. Подходы сильно рознятся, так что в некоторых странах даже запрещено использование компонентов или систем иностранного производства. Однако во многих странах энергетические компании не имеют возможности сделать покупку внутри страны, когда нужные устройства и приложения производятся исключительно за рубежом. В таких случаях предприятие должно выработать прагматичный подход к рискам, связанным с обеспечением и цепочкой поставок.

Одним из источников практических рекомендаций относительно рисков в цепочке поставок является документ Объединенного совета по телекоммуникациям *«Управление рисками цепочек поставок для энергетических компаний – план внедрения»* (Бартол, 2015). Ниже приведены основные выдержки данного документа (более подробную информацию и подробные объяснения можно найти в самой публикации):

- **Определите поставщиков, оцените их риски и расставьте приоритеты.** Это потребует определенных усилий, поскольку одно предприятие может зависеть от сотен разных поставщиков. Кроме того, каждый поставщик может включать детали и оборудование от многих субпоставщиков. Но как только предприятие определило своих основных поставщиков и субпоставщиков, оно может выявить тех из них, которые являются наиболее важными в разрезе кибербезопасности, либо из-за характера их продуктов, либо из-за объема доступа, который они будут иметь к системе предприятия во время сотрудничества. Наиболее важные поставщики и субпоставщики обладают наибольшим потенциалом воздействия, и им следует уделять больше внимания в процессе обеспечения.
- **Определить требования к безопасности и методы контроля их соблюдения.** Существует множество политик и стандартов, которые можно использовать в качестве основы для требований безопасности (например, стандарты защиты критической инфраструктуры Североамериканской корпорации по обеспечению надёжности электросетей или NIST). Энергетические компании могут попросить поставщиков самостоятельно подтвердить соблюдение данных политик и стандартов, или они могут использовать более строгий подход и проводить посещения объектов или проверки продуктов поставщиков. Самый строгий подход предполагает стороннее тестирование или сертификацию.
- **Подготовьтесь к прекращению сотрудничества с поставщиком.** В определенный момент предприятие может принять решение о смене поставщика по какой-либо причине. У предприятия должен быть план прекращения доступа поставщика к системам предприятия, когда этот доступ будет больше не нужен. Чем дольше продолжается сотрудничество с поставщиками, тем более осторожным и тщательным должно быть предприятие при его завершении.

Еще один ценный ресурс от Рабочей группы по системам контроля для энергетического сектора, *«Язык кибербезопасного обеспечения для систем энергоснабжения»* (Гофф, Гланц и Масселло, 2014 г.), приводит язык закупок в разрезе кибербезопасность. Язык закупок охватывает такие темы, как контроль доступа, ведение журналов и аудит, обнаружение вредоносных программ и методы безопасной разработки поставщика. Энергетические компании могут использовать этот язык и адаптировать его для контрактов с поставщиками, гарантируя, что они охватили все аспекты безопасности, относящиеся к закупаемому

продукту.

Ассоциация коммунального электроснабжения США и Национальная кооперативная ассоциация электрификации рекомендует рассылать стандартные анкеты по кибербезопасности поставщикам в качестве способа их проверки – возможно, на этапе запроса предложений («Управление рисками в цепочке поставок в киберпространстве – лучшие практики для малых предприятий» 2018). Они предоставляют темы для опросов (например, характер контроля доступа и безопасность управления информацией), но не содержат типовых вопросов. Однако такие образцы опросников можно найти на веб-сайтах консультантов (Келлер, 2020) или позаимствовать из других отраслей (Эрлунд, без даты).

8.4 Важная информация

Энергетические компании, стремящиеся улучшить свои процессы обеспечения, должны собрать следующую информацию:

- Список критических систем внутри предприятия, а также работающих в нем устройств, приложений и служб
- Список поставщиков, связанных с этими продуктами, сроки, в течении которых планируется сотрудничество с поставщиком
- Альтернативы для критических продуктов на случай, если поставщик прекратит производство или больше не будет производить или поддерживать критически важный продукт
- Инвентаризация всех поставщиков или продавцов, которые имеют доступ к системам предприятия, причины такого доступа и то, как этот доступ может быть приостановлен в случае необходимости
- Список источников информации о новых или существующих уязвимостях продукта и рекомендуемых действиях по исправлению

Рекомендованная литература и дополнительные источники по данному структурному блоку приведены приложении под заголовком «Обеспечение».

9 Технический контроль

Технический контроль – Компоненты оборудования и программного обеспечения, защищающие систему от кибератак. Брандмауэры, системы обнаружения вторжений (IDS), шифрование, механизмы идентификации и аутентификации являются примерами технических средств контроля (Харрис и Мэйми, 2016).

9.1 Важность

Технический контроль выполняют множество важных функций, таких как предотвращение несанкционированного доступа к системе и обнаружение нарушения безопасности. Поскольку эти функции так важны, некоторые люди думают, что технический контроль и есть вся кибербезопасность, игнорируя другие важные элементы (покрываемые другими структурными блоками).

Технический контроль должен быть организован таким образом, чтобы обеспечивать защиту как данных в состоянии покоя (например, данных, хранящихся на жестком диске), так и данных в движении (например, данных, перемещающихся по сети). Распространенным подходом к развертыванию элементов контроля является *многоуровневая защита*, при которой элементы контроля присутствуют на нескольких уровнях. В такой конфигурации если злоумышленник нарушает один элемент контроля, элементы контроля следующего уровня продолжают обеспечивать защиту.

9.2 Пересечение с другими структурными блоками

Структурный блок «**Политика безопасности организации**» определяет цели структурного блока «**Технический контроль**». Решения относительно того, какие средства контроля следует применить и как система контроля будет работать вместе (архитектура безопасности), принимает персонал, отвечающий за технический контроль. Ввиду сложности развертывания технического контроля, в небольших энергетических компаниях с ограниченными ресурсами нередко можно наблюдать излишние меры безопасности в одних областях и недостаточные в других (Инграм и Мартин, 2017). Этой проблемы можно избежать, при условии, что политика безопасности организации устанавливает цели контроля, основываясь потребностях управление рисками и соблюдения, а также стратегии управления (см. структурные блока **«Управление рисками»**, «**Соблюдение норм»** и **«Управление»**). Это обеспечивает более сбалансированный подход к безопасности в масштабах всей организации, который может быть воплощен путем выборочного развертывания технического контроля безопасности.

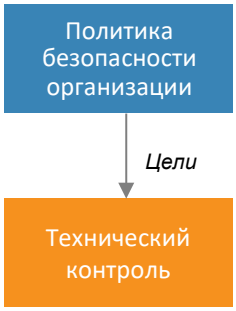


Рисунок 9. Входящая и исходящая информация структурного блока Технический контроль

9.3 Процессы и действия

Внедрение технического контроля включает в себя множество типов технологий и навыков, что затрудняет определение какого-либо одного действия в качестве единственно правильного «первого шага». Тем не менее, сетевая безопасность часто находится в авангарде многих работ по повышению безопасности. В 2020 году, когда Индия выпустила новые требования безопасности для энергетического сектора, межсетевые экраны были названы в качестве примера требуемого типа защитных устройств (T&D World, 2020). Частично это было ответом на заражение вредоносным ПО индийского производителя атомной энергии (Сингх, 2019).

Современное предприятие, вероятно, использует несколько сетей одновременно, включая корпоративную сеть, поддерживающую бизнес-функции и офисные функции (например, учет и электронную почту), и сеть системы телеуправления и сбора данных (SCADA), которая контролирует и отслеживает сетевое оборудование (например, станция управления удаленного доступа). По мере роста использования передовой измерительной инфраструктуры, интеллектуальных счетчиков и распределенных энергоресурсов (например, солнечная энергия, принадлежащая потребителю), энергетическим компаниям нужно расширять глобальные сети в полевых условиях для сбора данных и мониторинга состояния энергосистемы.

Сетевая безопасность включает в себя множество различных функций (больше, чем можно покрыть данными стандартными структурными блоками). Особого внимания заслуживают две из них: *контроль доступа* и мониторинг сети. Контроль доступа – это технологии, которые определяют, кто может подключаться к сети или системе, и что они могут делать при подключении. Пароль – это пример контроля доступа, в частности, пароли относятся к *аутентификации*, подтверждающей, что человек, устройство или приложение, которые хотят подключиться к сети, действительно являются тем, кем они себя называют. Только вы должны знать свой пароль, поэтому любой, кто знает ваш пароль, считается вами.

Контроль доступа в корпоративных сетях считается само собой разумеющимся (для работы вы каждый день входите в систему со своим паролем). Но по мере того, как SCADA и глобальные сети расширяются и приближаются к границе сети, контроль доступа становится актуальным и там.

Инструменты *мониторинга сети* обнаруживают подозрительную активность или трафик в сети. Эти инструменты обычно работают либо через обнаружение сигнатур, либо через обнаружение аномалий. Обнаружение сигнатур ищет данные, которые, как известно, связаны с определенным вредоносным ПО, в то время как обнаружение аномалий ищет все необычное, что «выглядит подозрительно». Хотя на рынке существует множество коммерческих инструментов для мониторинга сети, существуют также высококачественные альтернативы с открытым исходным кодом (Дролет, 2018). Ниже приведены три примера:

- **Snort** легко настраивается. Пользователи могут указать ему, что искать в сети и какие действия предпринимать при обнаружении угрозы.
- **Zeke** анализирует сетевой трафик. Его возможности создания сложных сценариев могут автоматизировать работу по реагированию на угрозы, но для этого требуется освоить новую технологию.
- **Kismet** обнаруживает вторжения в беспроводные сети, включая Wi-Fi и Bluetooth. Его можно использовать для отслеживания неавторизованных точек доступа, что помогает в контроле доступа.

Потребности безопасности сетей SCADA несколько отличаются от корпоративных сетей. Поскольку они контролируют устройства и процессы в физическом мире, необходимо проявлять особую осторожность при реагировании на предполагаемые кибер-вторжения, чтобы ответные действия не вызывали непредвиденных последствий в контролируемых физических системах. (Например, перед отключением генерирующей станции, которая может быть затронута вредоносным ПО, подумайте, может ли это вызвать веерное отключение.) Энергетические компании должны изучить особые требования, связанные с безопасностью SCADA.

Пункты ниже были выбраны и адаптированы из публикации *«21 шаг к повышению кибербезопасности сетей SCADA»* (Директива Президентской политики США, Безопасность и устойчивость критической национальной инфраструктуры 2002). Больше информации вы найдете в самой публикации, также многие из не включённых здесь шагов, разъясняются в других структурных блоках. Многие элементы в списке также можно применить к корпоративным сетям.

- **Максимально изолируйте сеть SCADA.** Найдите все точки соприкосновения между сетью SCADA и собственными локальными сетями предприятия, Интернетом или сетями, которые используют другие организации. Сюда могут входить беспроводные маршрутизаторы, спутниковые каналы или модемы коммутируемого доступа. Отключите как можно больше таких точек взаимодействия. Например, если точка взаимодействия используется нечасто и существует только для того, чтобы некоторым сотрудникам было удобно подключаться, рассмотрите возможность ее устранения. Остальные точки взаимодействия должны быть усилены межсетевыми экранами, IDS или другими подобными средствами защиты.
- **Отсоедините ненужные устройства и службы от сети SCADA.** Чем больше устройств, тем больше точек для кибератак. Завершение работы или удаление ненужных служб и устройств – недорогой способ защиты сети.
- **Используйте все возможные функции безопасности устройств и систем.** Некоторые устройства и системы могут иметь встроенные функции безопасности (например, шифрование или аутентификацию), но они не всегда используются, поскольку для этого может потребоваться дополнительная работа персонала. Изучение технической документации на эти устройства и, если возможно, их активация – еще один недорогой способ повысить безопасность.
- **Примените IDS.** IDS сканирует известные вредоносные программы или отслеживает сетевой трафик на предмет аномалий. Snort, Bro и Kismet являются примерами сетевых IDS с открытым исходным кодом, а OSSEC – пример IDS с открытым исходным кодом «на основе хоста» (Дролет, 2018).
- **Создайте «красную команду» для определения возможных сценариев атак SCADA.** «Красная команда» – это группа, которой поручено находить уязвимости в системе. Красные команды могут работать на подряде (например, для проведения теста на проникновение) или сотрудниками другого отдела в рамках организации. В идеале в красные команды не должны входить сотрудники, отвечающие за безопасность системы – идея состоит в том, чтобы по-новому взглянуть на состояние безопасности системы.
- **Проверяйте физическую безопасность удаленных блоков, которые подключены к сети SCADA.** Физический доступ к устройству или блоку может предоставить возможности для киберкомпрометации. Если потенциальный злоумышленник имеет неконтролируемый физический доступ к устройству, у

него есть хорошие шансы в конечном итоге обойти киберзащиту.

9.4 Важная информация

Энергетические компании, которые стремятся усилить Технический контроль своих сетей, должны собрать следующую информацию:

- Подробная информация о точках соприкосновения сети SCADA с другими сетями, включая корпоративную сеть предприятия и Интернет.
- Данные о физической безопасности удаленных объектов с доступом SCADA
- Данные системы управления по устройствам в системе и службам, которые они запускают.
- Информация о функциях безопасности, встроенных в устройства, подключенные к сети SCADA.
- Хранилища ценных данных в корпоративных сетях и сетях SCADA, а также технический контроль, используемый для их защиты.

Рекомендованная литература и дополнительные источники по данному структурному блоку приведены приложении под заголовком «Технический контроль».

10 Мероприятия по реагированию

Даже самые изощренные средства защиты могут быть взломаны злоумышленниками с достаточными навыками и ресурсами. Когда это произойдет, инцидент будет гораздо масштабнее, если защитники не спланировали и не отрепетировали стратегию реагирования. Действия, предпринимаемые организацией для подготовки к кибератаке и реагирования на нее, представляют собой *мероприятия по реагированию.*

10.1 Важность

Реагирование на киберинцидент – сложный и важный процесс. Даже в самых лучших обстоятельствах период после атаки будет хаотичным, поскольку персонал будет пытаться понять, что произошло, почему это произошло, как повлияло на бизнес и как наилучшим образом восстановить бизнес-функции. Энергетические компании должны заранее подготовить свои ответные реакции, в противном случае кибератака, вероятно, продлится дольше и нанесет больший ущерб, пока персонал предприятия будет пытается сформулировать определенный ответ. Активная подготовка к атаке посредством планирования, обучения и репетиций уменьшит хаос и степень воздействия атаки.

Не смотря на то, что данный структурный блок «**Мероприятия по реагированию»** прописан с акцентом на предприятии, его в равной степени можно применить и правительственным организациям, частным, некоммерческим и другим типам компаний. Организации любого типа извлекут выгоду из планирования мероприятий по реагированию, при неизбежной материализации атаки.

10.2 Пересечение с другими структурными блоками

Структурный блок **«Политика безопасности организации»** определяет некоторые главные цели мероприятий по реагированию и содержит ответы на некоторые главные вопросы. Роли и обязанности в рамках мероприятий по реагированию? Какой отдел отвечает за планирование мероприятий по реагированию в организации? Кто имеет право инициировать действие по реагированию? Какие ресурсы использовать для мероприятий по реагированию? Кому организация сообщает данные об атаке? Ответы на эти вопросы послужат основой для плана мероприятия по реагированию.

В зависимости от организации, может иметь смысл включить в политику безопасности только наиболее важны аспекты, касающиеся мероприятий по реагированию, и зафиксировать детали более низкого уровня в отдельной *политике мероприятий по реагированию*, которую можно будет обновлять более часто. Как минимум, политика безопасности организации должна включать заявление об обязательствах руководства и описание организационной структуры в поддержку мероприятий по реагированию.

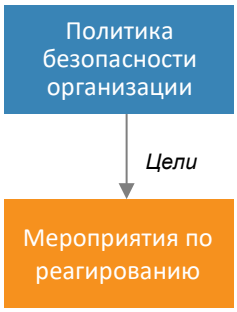


Рисунок 10. Входящая и исходящая информация структурного блока Мероприятия по реагированию

10.3 Процессы и действия

Пункты ниже являются адаптацией и кратким изложением публикации *«Руководство по обработке инцидентов компьютерной безопасности»* (Цихонськи и другие, 2012), которая содержит расширенную информацию по каждому пункту. Руководство рекомендует создать документы о политике, планах и процедурах мероприятий по реагированию и содержит перечисление элементов, которые следует включить в каждый из них. Политика является наиболее стратегической из трех, в то время как документ о процедурах является наиболее тактическим. Небольшие энергетические компании или компании, которые только начинают внедрять мероприятия по реагированию, могут объединить все три документа в один с разделами, посвященными политике, планированию и процедурам.

При подготовке к разработке данных документов предприятию потребуется собрать или создать следующую информацию:

- Список всех действующих законов, нормативных актов и стандартов, которые касаются мероприятий по реагированию и применятся к предприятию. Какие бы действия ни предусматривались такими законами, нормативными актами и стандартами, они должны быть включены в документы по реагированию. Возможны различия в зависимости от страны. Энергетические компании должны включать не только законы, нормативные акты и стандарты, характерные для сектора предприятий, но также законы, нормативные акты и стандарты, относительно конфиденциальности, защиты потребителей и т.д. Регулирующие органы должны предоставлять полезную информацию по этим темам.
- Определение терминов, относящихся к мероприятиям по реагированию, которые будут использованы в документах мероприятия по реагированию. Например, предприятие может дать определение «инцидент» кибербезопасности в соответствии со своими собственными критериями.
- Сопоставление департаментов и офисов предприятия с ролями, обязанностями и уровнями полномочий, которые они будут выполнять в мероприятиях по реагированию. Например, кто на предприятии имеет право отключать оборудование, если есть подозрение, что оно взломано?
- Ранжирование инцидентов в зависимости от их возможного воздействия на предприятие.
- План взаимодействия в рамках мероприятия по реагированию, включая внутреннее взаимодействие по предприятию и взаимодействие с другими предприятиями (например, медиа, клиенты, продавцы программного обеспечения, регулирующие органы и организации, отслеживающие CTI).
- Контрольные списки, формы и процессы, которые будут использоваться во время мероприятий по реагированию (например, процедура хранения зараженных жестких дисков для последующего криминалистического анализа).

Предприятие должно определить инструменты, которые оно будет использовать для выявления киберинцидентов, например IDS, антивирусное программное обеспечение и анализаторы журналов регистрации. Данная информация содержится в структурном блоке «**Технический контроль».**

Документы мероприятия по реагированию раскрывают информацию о четырех этапах:

- **Подготовка.** Создание документа (-ов) о политике, плане и процедурах мероприятия по реагированию; репетиция плана и его улучшение на основании извлеченных уроков; сбор всего оборудования и программного обеспечения (резервные диски,

инструменты судебной экспертизы, принтеры и т. д.), необходимого для выполнения мероприятий по реагированию, и определение наилучшего места, где могут работать специалисты по реагированию на инциденты.

- **Обнаружение и анализ.** Мониторинг IDS, системных журналов и/или антивирусного программного обеспечения на предмет наличия индикаторов взлома; при обнаружении подозрительного инцидента – проверка инцидента и запуск процесса реагирования; сопоставление индикаторов компрометации с другими наблюдениями за работой сети, устройств и систем; расследование причин и потенциальных последствий киберинцидента для выработки наилучшего ответа.
- **Сдерживание, уничтожение и восстановление.** Выбор и внедрение стратегий по сдерживанию (действия, которые не позволят кибератаке распространиться на другие устройства или системы), уничтожение (процесс удаления вредоносного ПО из системы) и восстановление (процесс возврата системы к нормальному функционированию).
- **Работа после инцидента.** Сбор уроков, извлеченных из инцидента, улучшение процесса реагирования и анализ данных об инцидентах, с целью выявления какие слабые места в защите безопасности необходимо устранить.

Подробная информация приведена в публикации *«Руководство по обработке инцидентов компьютерной безопасности»* (Цихонськи и другие, 2012).

Блок 5:
Терминология Мероприятий по реагированию

Инцидент или *инцидент компьютерной безопасности* - это «нарушение или непосредственная угроза нарушения политик компьютерной безопасности, политик допустимого использования или методов стандартной защиты» (Цихонськи и другие, 2012).
Термин *«событие»* иногда используется в качестве синонима *инцидента*.
Однако событие – это более широкий термин, охватывающий все, что можно наблюдать в системе (например, пользователь, отправляющий электронное письмо). События могут иметь или не иметь негативное влияние. Инциденты всегда имеют негативное влияние (Харрис и Мэйми, 2016).

10.4 Важная информация

Энергетические компании, планирующие создать или изменить план мероприятий по реагированию, должны собрать следующую информацию:

- Список всех действующих законов, нормативных и стандартов, относящихся к мероприятиям по реагированию
- Список телефонов/контактов, которым будут пользоваться сотрудники предприятия для оповещения друг друга при объявлении инцидента
- Список внешних сторон, которыми предприятие захочет общаться во время мероприятия по реагированию. Сюда могут входить СМИ, клиенты, поставщики программного обеспечения, правоохранительные органы и поставщики интернет-услуг
- Записи о лицензиях на программное обеспечение
- Расположение резервных копий данных и системы и процедуры восстановления из резервной копии
- Расположение оборудования и инструментов, которые будут использоваться во время мероприятия по реагированию.

Рекомендованная литература и дополнительные источники по данному структурному блоку приведены приложении под заголовком «Мероприятия по реагированию».

11 Обучение основам кибербезопасности

Чтобы предотвратить кибератаки, все сотрудники предприятия должны знать основные правильные привычки, способствующие кибербезопасность – то, что специалисты по безопасности называют *кибергигиеной*. По этой причине энергетические компании должны обучать своих сотрудников потенциальным угрозам и разъяснять их роли в предотвращении таких угроз. Такое обучение часто называют *обучением основам кибербезопасности*.

11.1 Важность

Успешность кибератак часто зависит от человеческих ошибок. Многие компании и даже правительства стали жертвами вредоносного ПО из-за того, что неосведомленный сотрудник кликнул на зараженное вложение электронной почты или вставил зараженный USB-накопитель в компьютер, как это, вероятно, произошло, когда Stuxnet проник на иранский завод по обогащению урана. (Зеттер, 2014). Обучение основам кибербезопасности учит сотрудников избегать таких ошибок. Выработка хороших и безопасных компьютерных привычек (кибергигиена) часто может сохранить время и деньги, а также предотвратить невозможность реализации планов и ущерб репутации организации. Эти простые привычки чрезвычайно эффективны при ликвидации уязвимостей, с помощью которых злоумышленники могут получить доступ к корпоративным системам. Исследования показали, что значительная часть (19% - 36%) утечек данных может быть вызвана человеческим фактором. («Исследование стоимости утечки данных, 2017 г.», 2017 г.).

11.2 Пересечение с другими структурными блоками

Структурный блок **«Политика безопасности организации»** определяет цели структурного блока **«Обучение основам кибербезопасности»**. Обучение основам кибербезопасности уделяет большое внимание обучению кибергигиене всех сотрудников, при этом подготовка трудовых ресурсов обеспечивает повышение квалификации технического персонала. Такие технические специалисты могут помочь контролировать и обучать нетехнический персонал, что делает обучение основам кибербезопасности более эффективным.

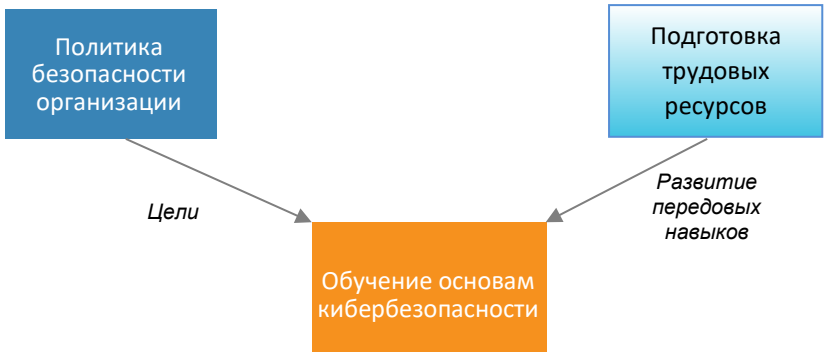


Рисунок 11. Входящая и исходящая информация структурного блока Обучение основам кибербезопасности

11.3 Процессы и действия

Сотрудники предприятие иногда считают, что ответственность за кибербезопасность лежит исключительно на ИТ-отделе. Сотрудники могут не знать, что их действия влияют на кибербезопасность или что они играют решающую роль в удержании кибератак от компьютеров и сетей предприятия.

Руководство должно внушить всем сотрудникам, что кибербезопасность – это приоритет организации и ответственность каждого. Нужно создать корпоративную культуру, которая определяет кибербезопасность в качестве ключевого элемент успеха организации. Руководство предприятия должно стремиться к формированию культуры кибербезопасности (Дролет, 2019). Персонал будет более открыт для изменений, если поймет, что вся иерархия ценит кибербезопасность и прилагает совместные усилия («Правда об обучении кибербезопасности», 2020 г.).

Обучение основам кибербезопасности работает наиболее эффективно в случае проведения базовых обучений на регулярной основе (например, однодневные занятия по кибербезопасности) (Харрис и Мэйми, 2016, 159). Закрепление материала может осуществляться через дополнительные занятия или онлайн-веб-семинары, викторины и упражнения по психологическим атакам. Под *психологическими атаками* следует понимать попытки злоумышленника заставить сотрудников вести кибер-небезопасное поведение. Одним из примеров этого является *фишинг*, при котором людей обманом заставляют кликнуть на вредоносную ссылку в электронном письме, придав ссылке законный вид.

Приемы психологических атак, используемые злоумышленниками, также могут быть использованы предприятием для обучения персонала противодействию таким приемам (например, сотрудники службы безопасности предприятия могут использовать фишинг для своих коллег). Цель этих упражнений должна заключаться в том, чтобы предоставить сотрудникам полезные обучающие упражнения, повысить их осведомленность о попытках атак в будущем. Наказание следует применять в ситуациях, когда сотрудник умышленно отказывается следовать рекомендациям по кибергигиене или постоянно становится потенциальным кибер-риском. («Правда об обучении кибербезопасности», 2020 г.).

Руководство должно мотивировать хорошее знание кибербезопасности. Ошибки сотрудников в области кибербезопасности обычно можно устранить с помощью дополнительного тренинга и обучения; иногда просто осведомленности о внутренних психологических атаках достаточно, чтобы мотивировать лучшее поведение. По возможности обучение основам кибербезопасности должно быть развлекательным, с юмором и простым для понимания (Харрис и Мэйми, 2016, 157). Цель состоит в том, чтобы сделать обучение достаточно длительным и превратить полезные кибер-навыки в своего рода мышечную память (Исследование Остермана, 2020).

Наконец, необходимо отслеживать осведомленность сотрудников о кибербезопасности, чтобы со временем увидеть рост осведомленности и соблюдение норм ожидаемого поведения.

11.4 Важная информация

Все сотрудники должны быть обучены базовым основам кибербезопасности. Сюда входит предотвращение фишинга, ответственное использование съемных носителей (например, USB-накопителей) и предотвращение использования незащищенных сетей Wi-Fi. Кроме того, некоторым сотрудникам, которые регулярно работают с конфиденциальной информацией, требуется дополнительное обучение. К конфиденциальной информации относится:

- Данные о деятельности и безопасности предприятия
- Персональная информация о клиентах и сотрудниках
- Финансовая информация
- Коммерческие тайны

- Любая информация, которая считается конфиденциальной в соответствии с местными законами или нормами
- Лицензии на программное обеспечение
- Подробная информация о конфигурациях компьютерной сети и другие данные, которые могут быть полезны для кибератак
- Информация, на которую распространяется соглашение о неразглашении, подписанное предприятием.

Поэтому важно знать, кто в организации имеет доступ к важным базам данных и файлам, чтобы определить тип необходимого обучения безопасности. При сборе данных можно ответить на такие вопросы:

- Кто имеет доступ к каждой категории важной информации?
- Как мы отслеживаем, у кого есть доступ к важной информации?
- Существует ли процесс отмены доступа к важной информации, когда она больше не нужна сотруднику или когда сотрудник увольняется из организации?
- Насколько важна эта информация? (Каким будет результат ее потери, кражи или изменения злоумышленником?)
- Что персоналу необходимо знать о безопасности каждого типа важной информации и о системе, в которой она хранится?
- Сбор этих данных позволит руководству предприятия определить потребности в обучении различных сотрудников.

Рекомендованная литература и дополнительные источники по данному структурному блоку приведены приложении под заголовком «Обучение основам кибербезопасности».

12 Подготовка трудовых ресурсов

Энергетическим компаниям необходимо, чтобы их ИТ-персонал, сотрудники службы безопасности и инженеры обладали специальными техническими знаниями в области кибербезопасности. Государственные учреждения могут помочь посредством программ *подготовки трудовых ресурсов*, которые обеспечивают обучение аспектам кибербезопасности.

12.1 Важность

Защита электросети от кибератак необходима для обеспечения безопасной и надежной работы этой критически важной инфраструктуры. Однако существует несоответствие между количеством квалифицированных специалистов по кибербезопасности в штате и нужным количеством специалистов. Международный консорциум по сертификации безопасности информационных систем оценивает нехватку квалифицированных специалистов по кибербезопасности в более чем 4 миллиона человек во всем мире («(ISC) 2 2019). Более того, энергетические компании конкурируют с другими отраслями – финансами, розничной торговлей, производством и т. д. - при найме на должности в сфере кибербезопасности.

Усилия по подготовке трудовых ресурсов делают образовательные ресурсы по кибербезопасности доступными для всех, кто хочет получить эти навыки. Программы подготовки трудовых ресурсов могут осуществляться национальными правительствами, некоммерческими организациями, энергетическими компаниями или любой другой организацией, заинтересованной в обеспечении достаточного количества специалистов по кибербезопасности.

12.2 Пересечение с другими структурными блоками

Структурный блок «**Подготовка трудовых ресурсов»** усиливает работы энергетической компании в рамках структурного блока **«Обучение основам кибербезопасности»**. В то время как обучение основам кибербезопасности затрагивает основные полезные навыки кибербезопасности, которые должны быть у всех сотрудников, подготовка трудовых ресурсов развивает те специализированные, всесторонние навыки кибербезопасности, которые необходимы ИТ-специалистам, специалистам по безопасности и инженерам. Такие технические специалисты помогают контролировать и обучать нетехнический персонал, делая обучение основам кибербезопасности более эффективным.

Рисунок 12. Входящая и исходящая информация структурного блока Подготовка трудовых ресурсов

12.3 Процессы и действия

Правительственным организациям следует рассмотреть способствование созданию программ по подготовке трудовых ресурсов на предприятиях как способ обеспечения достаточного количества специалистов кибербезопасности для всех отраслей, включая критическую инфраструктуру. Правительства могут даже рассматривать организацию таких программ.

Независимо от организатора, программа по подготовке трудовых ресурсов должна использовать наработки организаций относительно использования ними критически важной инфраструктуры в связи с потребностями в кибербезопасности и тех пробелов в навыках, которые они наблюдают у кандидатов на работу. Поскольку безопасность энергосистемы – вопрос национальной безопасности, оборонные или военные ведомства также могут внести свой вклад в определение целей обучения персонала. Затем ответственное государственное учреждение может проанализировать образовательные ресурсы внутри страны (университеты, профессиональные училища и т. д.), на базе которых могут быть созданы возможности для персонального или онлайн-обучения. Если оборонные или военные ведомства обладают достаточными ресурсами, они также могут проводить кибер-обучение гражданских лиц (включая персонал предприятия).

Возможность подготовки трудовых ресурсов также может быть предоставлена через коммерческие учреждения или даже иностранные правительственные агентства. План подготовки трудовых ресурсов в вопросах кибербезопасности должен быть составлен и рассмотрен всеми задействованными сторонами (обязательно учитывайте пробелы в навыках и бюджет). Государственные организации могут рассмотреть возможность мотивации лиц, уже работающих в критически важной инфраструктуре, повышать свои навыки в области кибербезопасности. Такая мотивация может быть предоставлены непосредственно отдельным лицам или работодателям их предприятий/критических инфраструктур или организациям, которые проводят учебные программы.

12.4 Важная информация

Будь то государственное учреждение, некоммерческая организация, университет или другое учреждение, любой, кто разрабатывает программу подготовки трудовых ресурсов, должен выяснить, есть ли у критически важных объектов инфраструктуры (таких как энергетические компании) в настоящее время доступ к следующим навыкам (либо через персонал или подрядчиков). Сбор этой информации позволит лучше сориентировать программу подготовки трудовых ресурсов на потребности критически важной инфраструктуры.

- Контроль доступа и управление учетными записями
- Сетевая безопасность и сегментация сети
- Действующие законы, нормативные акты и стандарты
- Требования безопасности, характерные для систем и сетей, необходимых для предоставления услуг (например, в энергетическом предприятии, сюда может входить безопасность систем SCADA).

Рекомендованная литература и дополнительные источники по данному структурному блоку приведены приложении под заголовком «Подготовка трудовых ресурсов».

Приложение A. Использованная литература и источники

Использованная литература и источники упорядочены в соответствии о структурными блоками, для которых они используются.

Часть приведенной ниже литературы и источников была опубликованы или спонсирована коммерческими компаниями по обучению основам кибербезопасности. Включение в этот список не означает одобрения издателя или спонсора.

Управление

Использованная литература

Бью Робин. «Пять принципов более строгого надзора за кибербезопасностью со стороны Совета директоров». BRINK - Новости и аналитическая информация о глобальных рисках. По состоянию на 5 января 2021 г.
https://www.brinknews.com/five- principles-for-stronger-board-oversight-of-cybersecurity/.

Национальная ассоциация корпоративных директоров. 2020. *«Руководство директора по контролю над киберугрозами NACD».*
https://www.nacdonline.org/insights/publications.cfm?ItemNumber=67298.

NIST (Национальный институт стандартизации и технологий). 2018. «Концепция повышения кибербезопасности критических объектов инфраструктуры, версия 1.1».
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

NREL (Национальная лаборатория по исследованиям в области возобновляемых источников энергии). «Структура кибербезопасности распределенных энергетических ресурсов». По состоянию на 5 января 2021г.
https://dercf.nrel.gov/.

Ротрок Рэй А., Джеймс Каплан и Фризо Ван дер Оорд. «Роль Совета директоров в управлении рисками кибербезопасности». *Обзор управления MIT Sloan*. 16 ноября 2017 г.
https://sloanreview.mit.edu/article/the-boards-role-in-managing-cybersecurity-risks/.

Tyler Cybersecurity. «Обучение кибербезопасности для руководителей и советов директоров». По состоянию на 5 января 2021 г.
https://www.tylercybersecurity.com/services/executive-cybersecurity-readiness-program.

Дополнительные источники

ANSI Webstore. «ISO/IEC 38500:2015 «Информационные технологии. Стратегическое управление ИТ в организации». По состоянию на 4 января 2021 г.
https://webstore.ansi.org/Standards/ISO/ISOIEC385002015?gclid=EAIaIQobChMImNnrn6SD7gIVBK-GCh38NQ8jEAAYASAAEgLCe_D_BwE.

Аткинсон Шон. «Преодоление разрыва между управлением и оперативной кибербезопасностью». Центр Интернет-безопасности. 10 апреля 2018 г.
https://www.cisecurity.org/blog/breaking-the- divide-between-governance-and-operational-cybersecurity/.

Бодо Деб, Стив Бойл, Дженн Фабиус-Грин и Рич Граубарт. 2010 г. *«Управление кибербезопасностью: составляющая методологии киберподготовки MITRE».* Корпорация

MITRE. https://www.mitre.org/sites/default/files/pdf/10_3710.pdf.

Берк Брэндон. «Управление и соблюдение норм». 3 апреля 2019 г. http://community.aiim.org/blogs/brandon-burke/2019/04/03/governance-vs-compliance.

Агентство кибербезопасности и безопасности инфраструктуры. «Управление кибербезопасностью | CISA ». 27 октября 2020 года. https://www.cisa.gov/cybersecurity-governance.

Educause. «Управление информационной безопасностью». По состоянию на 4 января 2021 г. https://library.educause.edu/topics/cybersecurity/information-security-governance.

Фонтейн Дэвид и Джон Старк. «Кибербезопасность: тревожный сигнал SEC для корпоративных директоров». Форум Гарвардской школы права по корпоративному управлению (блог). 31марта 2018 г. https://corpgov.law.harvard.edu/2018/03/31/cybersecurity-the-secs-wake-up-call-to-corporate-directors/.

Суинтон Сет и Стефани Хеджес. «Управление кибербезопасностью, фундаментальные проблемы, часть 1:5». Блог инсайдерских угроз (блог). 25 июля 2019 г. https://insights.sei.cmu.edu/insider-threat/2019/07/cybersecurity-governance-part-1-5-fundamental-challenges.html.

Велтсос Кристоф. «Совет директоров должен участвовать в управлении кибер-рисками». Разведка безопасности. 24 августа 2017 г. https://securityintelligence.com/board-directors-need-to-get-involved-with-cyber-risk-governance/.

Политика безопасности организации

Использованная литература

Харрис Шон и Фернандо Миими. 2016. *«Универсальное руководство для экзамена по профессиональной безопасности информационных систем»,* 7-е изд. Нью-Йорк: Образование Макгроу Хилл.

Ки Чай. 2001. Дорожная карта политики безопасности - процесс создания политик безопасности. Институт SANS. https://www.sans.org/reading-room/whitepapers/policyissues/security-policy-roadmap-process-creating-security-policies-494.

SANS. «Шаблоны политики безопасности». По состоянию на 30 декабря 2020 г. https://www.sans.org/information-security-policy/.

Дополнительные источники

Дуйган Адриан. «10 шагов к успешной политике безопасности». Компьютерный мир. 8 октября 2003 г. https://www.computerworld.com/article/2572970/10-steps-to-a-successful-security-policy.html.

Центр знаний IBM. «Разработка политики безопасности». 24 октября 2014 г. www.ibm.com/support/knowledgecenter/ssw_ibm_i_74/rzamv/rzamvdevelopsecpol.htm.

Национальный центр статистики образования. 2020. «Глава 3 - Политика безопасности: разработка и внедрение». *В защите вашей технологии: практические рекомендации по информационной безопасности электронного образования*. https://nces.ed.gov/pubs98/safetech/chapter3.asp.

Иевин Люк. «Как написать политику информационной безопасности - на примере шаблона». Блог по управлению ИТ En. 4 июня 2020 г. https://www.itgovernance.eu/blog/en/how-to-write-an-information-security-policy-with-template-example.

Нг Синди. «Как создать хорошую политику безопасности». безопасность наизнанку (блог). 29 марта 2020 г. https://www.varonis.com/blog/how-to-create-a-good-security-policy/.

Вуд Чарльз Крессон. 2002. *«Политика информационной безопасности простыми словами, 9-е изд.»* Технологии безопасности PentaSafe.

Управление рисками

Использованная литература

Министерство энергетики США. 2012. *«Процесс управления рисками кибербезопасности в энергетическом подсекторе».* DOE/OE-0003. https://www.energy.gov/ceser/downloads/cybersecurity-risk- management-process-rmp-guideline-final-may-2012.

Дополнительные источники

Пате-Корнелл, М.-Элизабет, Маршал Кайперс, Мэтью Смит и Филип Келлер. «Управление кибер-рисками критически важной инфраструктуры: модель анализа рисков и три тематических исследования». *Анализ рисков* 38, вып. 2 (2018): 226–41. https://doi.org/10.1111/risa.12844.

Устойчивая энергетическая платформа. «Рассчет риски». По состоянию на 5 января 2021 г. https://resilient-energy.org/guidebook/calculate-risks.

Уэстби Джоди и Лесли Лэмб. «Переосмысление риска в постпандемическом мире - управление рисками». Управление рисками. 1 декабря 2020 г. http://www.rmmagazine.com/2020/12/01/rethinking-risk-in-a-post-pandemic-world/.

Разведка в области киберугроз

Использованная литература

ENISA (Европейское агентство по сетевой и информационной безопасности). 2013. *«Картина угроз интеллектуальной энергосистемы и руководство по передовой практике».* https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide.

Метивье Бекки. 2016. «Руководство по источникам информации о киберугрозах». Tyler Cybersecurity. 12 июля 2016 г. https://www.tylercybersecurity.com/blog/guide-to-cyber-threat-intelligence- sources.

Группа анализа угроз. «Угроза, уязвимость, риск - часто смешанные термины». Группа анализа угроз (блог). 3 мая 2010 г. https://www.threatanalysis.com/2010/05/03/threat- vulnerability-risk-commonly-mixed-up-terms/.

Дополнительные источники

Андерсон Чад. 2020. «5 простых шагов для обеспечения обмена информацией о киберугрозах в вашей организации». Хелп Нет Секьюрити (блог). 21 сентября 2020 г. https://www.helpnetsecurity.com/2020/09/21/5-simple-steps-to-bring-cyber-threat-intelligence-sharing-to-your-organization/.

Крацдстрайк. 2020. *«Анализ угроз, тщательно хранимый секрет кибербезопасности».* https://go.crowdstrike.com/rs/281-OBQ-266/images/WhitepaperThreatIntelligence.pdf.

ENISA (Европейское агентство по сетевой и информационной безопасности). «Картина угроз ENISA – 2020». Тема. По состоянию на 15 декабря 2020 г. https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends.

Гуэрчио Кайл. «Лучшие платформы для сбора информации об угрозах на 2021 год | Планета электронной безопасности». По состоянию на 18 декабря 2020 г. https://www.esecurityplanet.com/products/threat-intelligence-platforms/.

Харрис Кевин. «Меняющаяся картина угроз современной кибербезопасности». *Безопасность*. 16 сентября 2020 г. https://www.securitymagazine.com/articles/93367-the-changing-threat-landscape-in- todays-cybersecurity?v=preview.

Джонс Шерри. «Угроза, уязвимость и риск: в чем различие?» Взаимодействие. 31 марта 2020 г. https://reciprocitylabs.com/threat-vulnerability-and-risk-whats-the-difference/.

Министерство внутренней безопасности США. «Понимание картины угроз». По состоянию на 15 декабря 2020 г. https://uscert.cisa.gov/sites/default/files/c3vp/smb/Understanding_the_Threat_Landscape.pdf.

Законы, нормативные акты и стандарты

Использованная литература

«IEEE 802.11». 2020. Стандарт. Институт инженеров по электротехнике и радиоэлектронике. https://standards.ieee.org/standard/802_11-2020.html.

Кио, Майлз и Пол Стек. 2017. *«Рамочные принципы оценки киберпространства для регуляторов в районе Черного моря».* https://pubs.naruc.org/pub.cfm?id=E3CE75B5-155D-0A36-31FD-1B268F7BD125.

Рагацци Елена, Альберто Стефанини, Даниэле Бенинтенди, Уго Финарди и Деннис К. Холстейн. 2020. Публикация *«Оценка обоснованности инвестиций в кибербезопасность. Методические указания для органов регулирования энергетики».* Национальная ассоциация контролёров коммунальных предприятий. https://pubs.naruc.org/pub.cfm?id=9865ECB8-155D-0A36-311A-9FEFE6DBD077.

Дополнительные источники

Финдлоу. «В чем разница между законами и нормативными актами?». По состоянию на 18 декабря 2020 г. https://blogs.findlaw.com/law_and_life/2015/10/whats-the-difference-between-laws-and-regulations.html.

Кио Майлз и Шэрон Томас. 2017. *«Основные принципы для государственных органов регулирования коммунального хозяйства».* Национальная ассоциация контролёров коммунальных предприятий https://pubs.naruc.org/pub/66D17AE4-A46F-B543-58EF-68B04E8B180F.

Массачусетская ассоциация консультантов по психическому здоровью. «В чем разница между законами и нормативными актами?». По состоянию на 18 декабря 2020 г. http://www.mamhca.org/assets/1/7/Laws_vs_regulations.pdf.

NARUC (Национальная ассоциация уполномоченных органов по регулированию коммунального хозяйства) «Регуляторная стратегия кибербезопасности: ключевой структурный блок основ политики кибербезопасности энергетического сектора». По состоянию на 13 мая 2020 г. https://www.naruc.org/international/news/the-regulatory-cybersecurity-strategy-a-key-building-block-for-an-energy-sector-s-cybersecurity-policy-framework/.

Сингх Раджеш Кумар. *«Индия планирует ввести обязательные меры кибербезопасности для электрических сетей».* The Economic Times. 21 января 2020.https://economictimes.indiatimes.com/industry/energy/power/india-plans-to-mandate-cyber-security-measures-for-power-grids/articleshow/73479609.cms?from=mdr.

Уолстром Майкл. «Интеллектуальная электрическая сеть Индии: проблемы институциональной и нормативной кибербезопасности». Школа международных исследований Генри М. Джексона (блог). 16 ноября 2016 г. https://jsis.washington.edu/news/indias-electrical-smart-grid-institutional-regulatory- cybersecurity-challenges/.

Соблюдение норм

Использованная литература

Уэст Курт. «5 лучших практик для соблюдение норм для предприятия: как избежать нормативных нарушений». Utility Cloud. 20 октября 2019 г. https://www.utilitycloud.us/blog/best-practices-utility- compliance-avoid-regulatory-violations.

Уоркентин Брэндон. «Самый крупный штраф NERC CIP на сегодняшний день: что вам нужно знать». Forescout (блог). 2 февраля 2019 г. https://www.forescout.com/company/blog/largest-nerc-cip-fine-to- date/.

Дополнительные источники

Берк Брэндон. «Управление и соблюдение норм.» 3 апреля 2019 г. http://community.aiim.org/blogs/brandon-burke/2019/04/03/governance-vs-соблюдение норм.

Обеспечение

Использованная литература

Американская ассоциация государственной энергетики и Национальная ассоциация сельских кооперативов по производству электроэнергии. 2018. *«Управление рисками в цепочке поставок в киберпространстве - оптимальные методы для малых предприятий».* https://www.cooperative.com/programs-services/government-relations/regulatory-issues/Documents/Supply%20Chain%20White%20Paper%204-25%20Final.pdf.

Бартол Надя. 2015. *«Управление рисками цепочки поставок в киберпространстве для коммунальных предприятий - Дорожная карта внедрения»*. Utilities Telecom Council.. https://utc.org/wp- content/uploads/2018/02/SupplyChain2015-2.pdf.

Эрлунд Андреас. «Кибербезопасность начинается с запроса предложения: 7 советов по обеспечению безопасности данных». Радиологический бизнес. По состоянию на 16 июля 2020 г. https://www.radiologybusiness.com/sponsored/1068/topics/privacy-security/cybersecurity-starts- rfp-7-tips-keep-data-safe.

Гофф Эд, Клифф Гланц и Ребекка Масселло. 2014. «Язык кибербезопасности для систем доставки энергии». *В материалах 9-й ежегодной конференции по исследованиям в области кибербезопасности и информационной безопасности - CISR* 14, 77–79. Ок-Ридж, Теннесси: ACM Press. https://doi.org/10.1145/2602087.2602097.

Харрис Шон и Фернандо Миими. 2016. *«Универсальное руководство для экзамена по профессиональной безопасности информационных систем»,* 7-е изд. Нью-Йорк: Образование Макгроу Хилл.

Келлер Джоэл. «10 самых распространенных вопросов в анкетах поставщиков по кибербезопасности». Venminder. 22 января 2020 г. https://www.venminder.com/blog/top-10-questions-vendor-cybersecurity- questionnaires.

Дополнительные источники

Бартол Надя. «ДНК практик безопасности киберпоставок - решение головоломки с использованием разнообразного набора дисциплин». Техновация 34, вып. 7 (2014): 354–61. https://doi.org/10.1016/j.technovation.2014.01.005.

Бойенс Джон М., Селия Полсен, Рама Мурти и Надя Бартол. 2015. «Практика управления рисками для федеральных информационных систем и организаций». NIST SP 800-161. Национальный институт стандартов и технологий. https://doi.org/10.6028/NIST.SP.800-161.

Хаас Джереми и Райан Бергквист. «Пять вопросов о сторонних поставщиках и кибербезопасности». SupplyChainBrain. 19 ноября 2019 г. https://www.supplychainbrain.com/blogs/1-think-tank/post/30489-the-company-you-keep-five-questions-to-ask-about-third-party-vendors-and-cybersecurity.

Уистик. «Запрос предложений: введение стандартов информационной безопасности и кибербезопасности в запросы предложений». Медиум. 16 января 2019 г. https://blog.whistic.com/rfps-introducing-information-security-cybersecurity-standards-in-rfps-abeddb80ced9.

Технический контроль

Использованная литература

Дролет Мишель. «5 инструментов обнаружения вторжений с открытым исходным кодом, которые нельзя игнорировать». Towerwall (блог). 19 октября 2018 г. https://towerwall.com/5-open-source-intrusion-detection-tools-that-are-too-good-to-ignore/.

Харрис Шон и Фернандо Миими. 2016. *«Универсальное руководство для экзамена по профессиональной безопасности информационных систем»,* 7-е изд. Нью-Йорк: Образование Макгроу Хилл.

Инграм Майкл и Морис Мартин. 2017. *«Руководство по кибербезопасности, устойчивости и надежности для малых энергетических компаний с ограниченными ресурсами»*. NREL/TP-5D00-67669. Национальная лаборатория возобновляемых источников энергии. https://energy.gov/sites/prod/files/2017/01/f34/Guide%20to%20Cybersecurity%2C%20Resilience%2C%20and%20Reliability%20for%20Small%20and%20Under-Resourced%20Энергетические компании.pdf.

Директива Президентской политики США Безопасность и устойчивость критической национальной инфраструктуры 2002. «21 шаг к повышению кибербезопасности сетей SCADA». Президентский совет по защите критически важной инфраструктуры и Управление энергетического обеспечения Министерства энергетики США. https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_- _SCADA.pdf.

Сингх Раджеш Кумар. «Индия утверждает, что атомная станция была заражена компьютерным вредоносным ПО». Блумберг. 31 октября 2019 г. https://www.bloomberg.com/news/articles/2019-10-31/india-says-nuclear-power-plant-was-

affected-by-computer-malware.

T&D World. «Индия планирует ввести обязательные меры кибербезопасности для электрических сетей». 22 января 2020 г. https://www.tdworld.com/smart-utility/grid-security/article/21121025/india-plans-to- mandate-cybersecurity-measures-for-power-grids.

Дополнительные источники

Гейтер Энди, Скотт Кинг, Даррен Беннет, Джошуа Карлсон, Шейн Маркли, Патрик Нортон, команда учебной программы ICS Института SANS, Тед Гэри и Коди Дюмон. нет даты *«Руководство по внедрению промышленных систем управления, версия 7».* Центр интернет-безопасности. https://www.cisecurity.org/white-papers/cis-controls-implementation-guide-for-industrial- control-systems/.

Обрегон Лучиана. 2015. *«Безопасная архитектура для промышленных систем управления».* Институт SANS. https://www.sans.org/reading-room/whitepapers/ICS/secure-architecture-industrial-control-systems-36327.

Стоуфер Кейт, Виктория Пиллиттери, Сюзанна Лайтман, Маршал Абрамс и Адам Хан. 2015. *«Руководство по безопасности промышленных систем управления (АСУ ТП)».* Специальная публикация NIST 800-82. Национальный институт стандартов и технологий. http://dx.doi.org/10.6028/NIST.SP.800-82r2.

Мероприятия по реагированию

Использованная литература

Чичонски Пол, Томас Миллар, Тим Гранс и Карен Скарфон. 2012. *«Руководство по обработке инцидентов компьютерной безопасности».* Специальная публикация NIST (SP) 800-61 Ред. 2. Национальный институт стандартов и технологий. https://doi.org/10.6028/NIST.SP.800-61r2.

Харрис Шон и Фернандо Миими. 2016. *«Универсальное руководство для экзамена по профессиональной безопасности информационных систем»,* 7-е изд. Нью-Йорк: Образование Макгроу Хилл.

Дополнительные источники

Краудстрайк. «Мероприятия по реагированию». По состоянию на 18 ноября 2020 г. https://www.crowdstrike.com/services/am-i-breached/incident-response/.

Разведка безопасности. «Мероприятия по реагированию». По состоянию на 17 апреля 2019 г. securityintelligence.com/category/incident-response.

Обучение основам кибербезопасности

Использованная литература

Дролет Мишель. «Семь советов для успешной программы обучения навыкам безопасности». *Forbes*. 16 августа 2019 г. https://www.forbes.com/sites/forbestechcouncil/2019/08/16/seven-tips-for-a- successful-security-awareness-training-program/.

Харрис Шон и Фернандо Миими. 2016. *«Универсальное руководство для экзамена по*

профессиональной безопасности информационных систем», 7-е изд. Нью-Йорк: Образование Макгроу Хилл.

Исследования Остерман. «Правда о тренингах по кибербезопасности». По состоянию на 10 декабря 2020 г. https://www.mimecast.com/globalassets/documents/whitepapers/wp_thetruth_cybersecuritytraining_osterman.pdf.

Институт Понемона. 2017. *«Исследование стоимости утечки данных за 2017 год».* https://www.ibm.com/downloads/cas/ZYKLN2E3.

Зеттер, Ким. 2014. *«Обратный отсчет до дня ноль»*. Нью-Йорк: Crown Publishers.

Дополнительные источники

Беделл Кристалл. «Первая линия защиты: достаточно ли хорошо люди делают свою работу?» InfoSecurity Professional. 14 мая 2020. https://blog.isc2.org/isc2_blog/2020/05/the-first-line-of-defense-are-humans-doing-a-good-enough-job.html.

Livingsecurity. «Погружающий обучающий контент по кибербезопасности для вовлечения сотрудников ... и продолжения их обучения». По состоянию на 11 декабря 2020 г. https://www.livingsecurity.com/products/cybersecurity-training-content.

Морган Стив. «Twitter отправляет своих сотрудников обратно в школу для обучения кибербезопасности». *Журнал Cybercrime* (блог). 18 июля 2020 г. https://cybersecurityventures.com/twitter-sends-its-employees-back-to-school-for-cybersecurity-training/.

Исследования Остерман. 2018. *«Лучшие практики защиты от фишинга, программ-вымогателей и мошенничества с электронной почтой».* https://www.knowbe4.com/hubfs/Best_Practices_for_Protecting_Against_Phishing_Ransomware_and_Email_Fraud.pdf?hsCtaTracking=67a14d06-dd12-49c7-8070- 93fa017a2729%7C082896ec-48d5-4248-b50b-a38e0076ee1a

Роуз Эшли. «Тренинг по вопросам безопасности: не обвиняйте своих сотрудников». Журнал Cybercrime (блог). 12 октября 2020 г. https://cybersecurityventures.com/security-awareness- training-dont-blame-your-employees/.

Трудовые ресурсы

Использованная литература

ISC2. «(ISC) 2 обнаруживает, что потребности в кадрах для кибербезопасности вырастут на 145%, чтобы ликвидировать пробелы в навыках и лучше защищать организации во всем мире». 6 ноября 2019 г. https://www.isc2.org:443/News- and-Events/Press-Room/Posts/2019/11/06/ISC2-Finds-the-Cybersecurity-Workforce-Needs-to- Grow--145.

www.resilient-energy.org | www.nrel.gov/usaid-partnership

Jeremy Foster
Агентство США по международному развитию Эл. почта: jfoster@usaid.gov

Sarah Lawson
Агентством международного развития США Эл. почта: slawson@usaid.gov

Sadie Cox
Национальная лаборатория по исследованиям в области возобновляемых источников энергии
Эл. почта: sadie.cox@nrel.gov

NREL/TP-5R00-79396 | Март 2021 г.

Платформа устойчивой энергетики предоставляет курируемые экспертами ресурсы, обучение, инструменты и техническую помощь для повышения устойчивости электроэнергетического сектора. Платформа устойчивой энергетики поддерживается Агентством международного развития США.

Партнерство AMP и NREL решает важнейшие задачи по расширению передовых энергетических систем с помощью глобальных инструментов и технической помощи, включая «Исследовательский инструмент данных по возобновляемым источникам энергии», «Экологическая направленность сети», «Международный инструмент воздействия на рабочие места и экономическое развитие», а также «Платформа устойчивой энергетики». Дополнительную информацию можно найти по адресу: **www.nrel.gov/usaid-partnership**.

USAID FROM THE AMERICAN PEOPLE

NREL Transforming ENERGY

REexplorer MAPPING OUR ENERGY FUTURE

Greening the Grid

I-JEDI

Resilient Energy Platform