Информационная безопасность

ООО «Эффективные технологии»

Цели организации ИБ

- минимизация рисков нарушения работоспособности ЭТП в рамках работ, проводимых сотрудниками ООО «Эффективные технологии»;
- минимизация рисков утечки «чувствительной» информации о торговых процедурах, об устройстве и функционировании ЭТП.

Цели обучения:

- Знание правил и стандартов работы;
- Повышение аккуратности в повседневной работе;
- Исключение критичных ошибок в организации работы.

Объекты защиты

- Основной корпоративный ресурс - ЭТП
- Защита конфиденциальной информации клиентов ЭТП;
- Доступность ЭТП для клиентов;
- Персональные данные клиентов;
- Исходный код;
- Реквизиты доступа к порталу и инструментам разработки;
- Документация: ТЗ, алгоритмы и прочие описания, информация об ошибках, средствах защит;
- Технические ресурсы: промышленный и тестовый контуры
- Офисная инфраструктура. Технические ресурсы: АРМ, офисная инфраструктура
- Собственная информация ограниченного доступа компании (персональные данные работников, коммерческая тайна: собственная и клиентов, прочая конфиденциальная информация).

Полный перечень защищаемой информации Оператора ЭТП приведен в документе: **Перечень сведений ограниченного доступа АО «ЭТС»** (Приложение №3 к «Положению о коммерческой тайне» от 05.08.2019).

Меры и ответственность

Для обеспечения ИБ ЭТП и компании разработаны и применяются **меры** защиты**,** которые базируются на законодательстве РФ (законы, требования регулирующих органов: ФСТЭК, ФСБ).

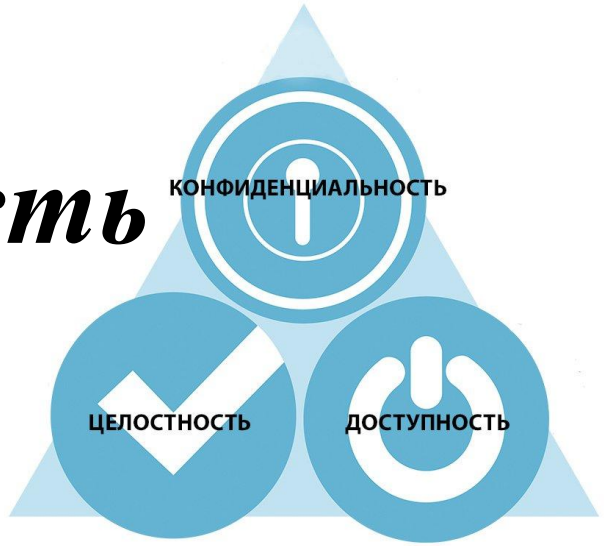
За нарушение мер предусмотрена **ответственность** – также в соответствии с законодательством РФ (трудовое, административное, уголовное).

Разглашение информации и иные нарушения:

- Умышленное
- Неумышленное

Деятельность пользователей может **наблюдаться, протоколироваться** и периодически **проверяться** на предмет соблюдения установленных правил работы любыми средствами, **не противоречащими законодательству** Российской Федерации.

Информационная безопасность



- это обеспечение конфиденциальности,

целостности и доступности информации

1. **Конфиденциальность** – доступность информации только определенному кругу лиц (авторизованные пользователи);
2. **Целостность** – неискаженность информации (эталон = исходная информация);
3. **Доступность** – беспрепятственный доступ к информации и средствам ее обработки того, кому это разрешено (авторизованным пользователям).

Конфиденциальность

1)Сохранение конфиденциальности информации (предотвращение разглашения)

Наравне с собственными данными ограниченного доступа, защите подлежат и данные, полученные от **контрагентов**.

Таким образом, являясь Подрядчиком, вы не вправе разглашать конфиденциальную информацию, которую предоставил Заказчик для выполнения работ.

Работа с документацией: считаем **всю** внутреннюю документацию конфиденциальной информацией, т.к. она часто содержит «чувствительную» информацию, вплоть до коммерческой тайны (простой принцип: все, что на работе - должно храниться и обрабатываться только в рамках рабочего процесса).

Хранение кода ЭТП, публикация рабочей документации во внешних системах, облачных сервисах запрещена.

Конфиденциальность

Не раскрывать информацию при публикации **статей, комментариев** на профильных сайтах (Хабр и т.д.). При использовании рабочих «кейсов» - обеспечить анонимность (компании, имен, адресов), заменять реальные куски кода «аналогами».

Сохранение конфиденциальности информации (“need to know”) при общении с коллегами (совещания, доклады, презентации).

Передача конфиденциальной информации контрагентам (иногда – и коллегам) по внешним каналам или вне рабочего контура (архивируем с паролем).

2) Идентификация и аутентификация

Разрешается работа только под **своей** личной (персональной) учетной записью.

Владелец учетной записи несет ответственность за **все** действия, совершенные от имени данной УЗ.

Запрещена работа под сервисными учетными записями (deploy, application и др.).

Запрещено разглашать реквизиты УЗ, ключи ssh.

Доступность

Нарушение работоспособности ЭТП или рабочей среды (ошибки специалистов при работе с промышленным контуром, ошибки в коде, вредоносное ПО)

- Скрипты, выполняемые на бою (перед релизом должно быть проведено ревью)
- Работа с БД (выполнение всех операций в тестовых контурах либо на репликах БД)

Регламент работы с базами данных промышленного контура https://confluence.fabrikant.ru/pages/viewpage.action?pageId=271847589

- Вредоносное ПО

- данные, полученные из сети Интернет (загрузка файлов с ресурсов с сомнительной репутацией, взломщики ПО, «пиратское» ПО, вложения в письма от неизвестных отправителей);

- стараться свести использование флешек к минимуму (потенциальная возможность занести вредоносное ПО в рабочие контура);

- использование антивирусных средств (участие работника в контроле, что САЗ функционирует, реакция на сообщения о вирусных инцидентах).

Целостность

- обеспечение достоверности и полноты «эталонности» информации;

Риски нарушения целостности связаны с выполнением работ с базами данных или файловыми хранилищами (релизы и выполнение скриптов).

Меры:

- Тщательное планирование релиза и строгое выполнение Workflow 2.0;
- Наличие плана отката и восстановления исходной информации и состояния системы;
- Реализация и использование процедуры отслеживания и исправления обнаруженных ошибок ПО и уязвимостей программы.

Доступ к активам

Принцип предоставления доступа

к информации - “need to know”

Доступ для работников организует руководитель.

Руководитель подразделения создает заявку в ПО Redmine, в проекте «Заявки на доступ» с обязательным указанием следующей информации:

- ФИО работника;
- Ресурс (наименование, IP адрес);
- Обоснование необходимости доступа
- Срок доступа

Redmine позволяет сформировать **шаблоны доступа** для подразделений (типовые наборы ресурсов для доступа по функциональным или должностным ролям, а так же на время испытательного срока)

Менеджеру

- **Работа с контрагентами**

Договор должен содержать раздел «Конфиденциальность»,

который обязателен к **согласованию** с ОИБ.

По решению ОИБ может быть инициировано подписание **Соглашения о конфиденциальности (NDA)** (Приложение №6 к Положению о коммерческой тайне).

- **Согласование проектов с отделами эксплуатации и ИБ.**

Регламент «Требования к описанию новых подсистем» (https://confluence.fabrikant.ru/pages/viewpage.action?pageId=271854185)

- «2.3. Информация о планах по внедрению новой подсистемы должна быть заблаговременно доведена до Отдела ИБ и Отдела эксплуатации, которые должны своевременно сформулировать вопросы, требования, риски, ограничения..»
- «2.4. Разворачивание компонентов подсистемы в продуктовом (промышленном) контуре возможно только после согласования всех аспектов с Отделом ИБ и Отделом эксплуатации...»
- «2.8. Возможность разворачивания новой подсистемы в продуктовом контуре должна быть явно подтверждена Отделом ИБ и Отделом эксплуатации.»

Правила удаленной работы

Подготовка ПК для удаленной работы:

- Создание отдельной учетной записи (УЗ),

её использование только для удаленной работы (УЗ не должна иметь права локального администратора);

- Установить пароль для всех УЗ на ПК (>=7 символов, пароли не должны совпадать с ранее используемыми паролями на других УЗ);
- Произвести установку обновлений безопасности ОС;
- Установить антивирусное ПО;
- Обеспечить отсутствие потенциально опасного ПО, в т.ч. ПО для удаленного управления ПК.

Правила удаленной работы

Запрещается

- Использовать для работы компьютеры, размещенные в общественных местах. Допускается использовать только личные устройства и только дома (ином «доверенном» месте)!
- Запрещается сохранять пароли для доступа к корпоративным ресурсам в ПО домашнего компьютера (браузеры, VPN и т.д.).
- Не посещать сайты, которые могут нести потенциальную опасность и риски заражения ПК вирусами (псевдо-новостные сайты, сайты с пиратским ПО и фильмами, порносайты и др.).

Меры, направленные на защиту от копирования ключевой и парольной информации

- Файл конфигурации удаленного доступа (****.ovpn), логины и пароли – это строго конфиденциальная информация. Никому, не при каких обстоятельствах не раскрывайте эти данные!
- При подозрениях на компрометацию (раскрытие посторонним лицам) файла конфигурации *.ovpn, логинов или паролей следует незамедлительно сообщить об этом в Отдел информационной безопасности через мессенджер WhatsApp, Битрикс или по телефону.

Работа с сертификатами

Регламент по обеспечению жизненного цикла сертификатов электронной подписи

https://confluence.fabrikant.ru/pages/viewpage.action?pageId=271847322

- ОИБ формирует реестр сертификатов https://confluence.fabrikant.ru/pages/viewpage.action?pageId=266641626
- ОИБ отслеживает сроки действия сертификатов и своевременно организует выпуск новых сертификатов и передачу в группы, поддерживающие соответствующие сервисы
- Менеджеры команд разработки организуют/выполняют (при наличии технической возможности) все необходимые работы по смене сертификата. Информируют ОИБ при необходимости выпуска дополнительных сертификатов для сервисов.
- Работники ОИС выполняют работы по смене сертификатов на АРМ, установке необходимого ПО (за исключением сертификатов финансовых приложений).

Персональная ответственность работника

- не разглашать, не передавать свои
- реквизиты доступа;
- не сохранять пароли в ПО;
- не отключать САЗ на АРМе;
- не делать «закладки» в коде;
- не публиковать фрагменты кода и информацию об уязвимостях;
- не выносить, не хранить вовне, не разглашать конфиденциальные материалы.

При возникновении вопросов, связанных с ИБ

- Обратиться с вопросом к непосредственному руководителю
- Обратиться в отдел информационной безопасности

Если Вы стали свидетелем нарушения ИБ, то обязаны незамедлительно сообщить об этом сотруднику ОИБ!!!

В случае компрометации пароля (ключа ssh, сертификата ЭЦП) или подозрений на компрометацию необходимо срочно сообщить об этом сотруднику ОИБ!!!

Отдел информационной безопасности

водитель отдела

трий Смирнов

26)721-33-85,

ant.ru

щий специалист

сим Анцыфров

60)160-28-88

cifrov@etpz.ru

Вопросы ?