ЕГЖЕЙ-ТЕГЖЕЙЛІ **ҚАУІПСІЗДІК**
БЕЗОПАСНОСТЬ В ДЕТАЛЯХ

АҚПАРАТТЫҚ **ҚАУІПСІЗДІК**

ИНФОРМАЦИОННАЯ **БЕЗОПАСНОСТЬ**

Ақпараттық қауіпсіздік - бұл кәсіпорынның деректері мен ақпараттық жүйелерін рұқсатсыз кіруден, ақпараттың жайылып кетуінен, жойылуынан немесе өзгеруінен қорғауға бағытталған шаралар кешені. Өндірістік үдерістерді заманауи цифрландыру жағдайында құпия ақпаратты қорғау компания қауіпсіздігінің негізгі аспектілерінің біріне айналуда.

АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІҢ НЕГІЗГІ МІНДЕТТЕРІНЕ МЫНАЛАР ЖАТАДЫ:
- Корпоративтік желіні сыртқы және ішкі қатерлерден қорғау;
- Деректердің тұтастығы мен құпиялылығын қамтамасыз ету;
- Ақпараттық ресурстарға қол жеткізуді бақылау;
- Кибершабуылдар мен вирустық қауіптердің алдын алу.

Ақпараттық қауіпсіздіктің жоғары дәрежесін сақтау үшін деректерді шифрлау жүйелері, антивирустық бағдарламалар және желілік белсенділікті бақылау жүйесі сияқты заманауи қорғаныс технологиялары қолданылады.
Оқыс оқиғаларды тудыруы мүмкін адами факторды азайту үшін ақпараттық ресурстармен жұмыс істеу ережелерін үнемі оқып отыру маңызды.
Ақпараттық қауіпсіздікті бұзу қаржылық шығындарға, бәсекелестік артықшылықтардың жоғалуына және компанияның беделіне нұқсан келтіруі мүмкін, сондықтан оны қамтамасыз ету компаниядағы тәуекелдерді басқарудың жалпы үдерісінің маңызды құрамдас бөлігі болып табылады.

Информационная безопасность — комплекс мер, направленных на защиту данных и информационных систем от несанкционированного доступа, утечки, уничтожения или изменения информации. В условиях современной цифровизации производственных процессов, защита конфиденциальной информации – один из ключевых аспектов безопасности компании.

ОСНОВНЫЕ ЗАДАЧИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВКЛЮЧАЮТ:
- Защиту корпоративной сети от внешних и внутренних угроз;
- Обеспечение целостности и конфиденциальности данных;
- Контроль доступа к информационным ресурсам;
- Предотвращение кибератак и вирусных угроз.

Для поддержания высокой степени информационной безопасности используются современные технологии защиты – системы шифрования данных, антивирусное ПО и система мониторинга сетевой активности.
Важно регулярно проходить обучение правилам работы с информационными ресурсами, чтобы минимизировать человеческий фактор, который может стать причиной инцидентов.
Нарушение информационной безопасности может привести к финансовым потерям, утрате конкурентных преимуществ и нанесению вреда репутации компании, поэтому её обеспечение является важной составляющей общего процесса управления рисками.

Ақпарат пен АТ ресурстарын қорғау

Қорғау объектілері: Құпия деректер (мәліметтер базасы, жүйелік құжаттама, оқу материалдары және электрондық ресурстар) негізгі қорғаныс объектілері болып табылады. Олар рұқсатсыз кіруден және кездейсоқ және қасақана кез келген әсерден қорғалуы керек.
АТ инфрақұрылымы: Ақпаратты өңдеу, беру және сақтау жүйелерін (байланыс арналары, телекоммуникациялар және деректер тасымалдаушылары) қамтиды. Оларды қорғау үшін корпоративті құралдар қолданылуы керек.
Мақсаты: Компанияның қауіпсіздігін қамтамасыз ету, рұқсатсыз кірудің зақымдануын болдырмау және деректердің құпиялылығын, тұтастығын және қол жетімділігін сақтау.

Защита информации и ИТ-ресурсов

Объекты защиты: Конфиденциальные данные (базы данных, системная документация, учебные материалы и электронные ресурсы) являются ключевыми объектами защиты. Они должны быть защищены от несанкционированного доступа и любых воздействий, как случайных, так и преднамеренных.
ИТ-инфраструктура: Включает системы обработки, передачи и хранения информации (каналы связи, телекоммуникации и носители данных). Для их защиты должны использоваться корпоративные инструменты.
Цель: Обеспечение безопасности компании, предотвращение ущерба от несанкционированного доступа и поддержание конфиденциальности, целостности и доступности данных.

Құпиясөз саясаты

Құпиясөзге қойылатын талаптар: Құпиясөздер әр түрлі регистрлердегі сандар мен әріптерді қамтитын кем дегенде 8 таңбадан тұруы керек.
Құпиясөздер әр 60 күн сайын және 48 сағатта бір реттен жиі жаңартылмауы керек.
Құпиясөзді өзгерткен кезде пайдаланушы алдыңғы үш құпиясөзді қайта пайдаланбауы керек.
Тіркелгі атауларын құпиясөз ретінде пайдалануға тыйым салынады.
Қауіпсіздік: Құпиясөздерді басқа қызметкерлерге беруге немесе қағазға жазуға болмайды.
Құпиясөздерді ашық сақтауға тыйым салынады.
Есептік жазбаларды бұғаттау: 5 сәтсіз авторизациядан кейін есептік жазба бұғатталады.
Құлыпты ашу үшін АТ бөліміне хабарласу қажет.
Апаттық жағдайлар: Егер оның бұзылуына күдік болса, құпиясөз дереу өзгертілуі керек.

Парольная политика

Требования к паролю: Пароли должны состоять минимум из 8 символов, включать цифры и буквы в разных регистрах.
Пароли должны обновляться каждые 60 дней и не чаще чем один раз в 48 часов.
При смене пароля пользователь не должен повторно использовать предыдущие три пароля.
Имена учетных записей запрещено использовать в качестве паролей.
Безопасность: Пароли нельзя передавать другим сотрудникам или записывать на бумаге.
Хранение паролей в открытом виде запрещено.
Блокировка учетных записей: После 5 неудачных попыток авторизации учетная запись блокируется. Для разблокировки требуется обращение в ИТ-отдел.
Аварийные ситуации: Пароль должен быть изменен немедленно, если есть подозрение на его компрометацию.

Антивирустық қорғаныс

Мониторинг және жаңартулар: Антивирустық бағдарламалар барлық құрылғыларда орнатылуы керек. Пайдаланушылар антивирустық қосымшаларды өшіруге немесе олардың параметрлерін өзгертуге құқылы емес. Антивирустық базалар күн сайын жаңартылып отырады.
Тұрақты тексерулер: Жұмыс станцияларын вирустарға толық тексеру айына кемінде бір рет жүргізіледі.
Бөгде БҚ тыйым салу: Корпоративтік стандарттардан бөгде антивирустық бағдарламаларын орнатуға және пайдалануға тыйым салынады.

Интернетпен жұмыс

Ресурстарға қол жеткізу: Ойын-сауық және зиянды сайттарға кіру бұғатталған. Интернетті пайдалану тек қызметтік қажеттіліктер үшін рұқсат етіледі.
Мақсатсыз пайдалануға тыйым салу: Компанияда пайдалануға рұқсат етілген тізімге кірмейтін бағдарламалық құралды жүктеп алуға және орнатуға, ақпараттық бюллетеньдерге жазылу немесе интернетті жеке қажеттіліктер үшін пайдалануға тыйым салынады.
Бақылау: Интернет-ресурстарға қол жетімділікті ақпараттық қауіпсіздік менеджері бақылайды.

Антивирусная защита

Мониторинг и обновления: Антивирусные программы должны быть установлены на всех устройствах. Пользователи не имеют права отключать антивирусные приложения или менять их настройки. Антивирусные базы обновляются ежедневно.
Регулярные проверки: Полные проверки рабочих станций на вирусы проводятся не реже одного раза в месяц.
Запрет на стороннее ПО: Установка и использование сторонних антивирусных программ, отличных от корпоративных стандартов, запрещена.

Работа с Интернетом

Доступ к ресурсам: Доступ к развлекательным и вредоносным сайтам заблокирован. Использование Интернета разрешено только для служебных нужд.
Запрет на нецелевое использование: Запрещено скачивать и устанавливать программное обеспечение, не входящие в список разрешенного к использованию в Компании. Подписываться на рассылки или использовать Интернет для личных нужд.
Контроль: Доступ к Интернет-ресурсам контролируется менеджером по информационной безопасности.

Электрондық поштаны пайдалану

Корпоративтік пошта: Электрондық пошта тек қызметтік мақсатта қолданылады. Құпия ақпаратты беру үшін сыртқы пошта қызметтерін пайдалануға тыйым салынады.
Сақтық шаралары: Корпоративтік пошта мекенжайын форумдарда, әлеуметтік желілерде немесе басқа қоғамдық ресурстарда жарияламаңыз. Жаппай қызметтік емес жіберулерге де тыйым салынады.
Күдікті хаттарды өңдеу: Тіркемелері бар белгісіз жіберушілердің хаттары дереу жойылуы керек. Күдікті хаттардың сілтемелеріне өтуге тыйым салынады.
Егер жолдаушы сізге хат жібердім деп мәлімдесе, бірақ сіз оны алмаған болсаңыз, сіздің бөлімшеңізге қызмет көрсететін жүйелік әкімшіге хабарласыңыз.

Использование электронной почты

Корпоративная почта: Электронная почта используется исключительно для служебных целей. Запрещено использовать внешние почтовые сервисы для передачи конфиденциальной информации.
Меры предосторожности: Не публикуйте адрес корпоративной почты на форумах, в социальных сетях или других общедоступных ресурсах. Массовые неслужебные рассылки также запрещены.
Обработка подозрительных писем: Письма от неизвестных отправителей, содержащие вложения, должны быть немедленно удалены. Запрещено переходить по ссылкам из подозрительных писем.
Если адресат утверждает, что отправил Вам письмо, но Вы его не получили, обратитесь к системному администратору обслуживающему Ваше подразделение.

Сыртқы тасушыны пайдалану

Ұсыныстар: Кәсіпорын деректерін тасымалдау және сақтау үшін компания ұсынған шифрланған сыртқы тасушыны ғана пайдаланыңыз.
Жеке деректерге тыйым салу: Қызметтік ақпаратты жеке тасушыларда сақтауға тыйым салынады.
Деректерді жою: Деректерді жұмыс станциясына көшіргеннен кейін ақпарат сыртқы тасушыдан жойылуы керек.

Қашықтан қол жеткізу

VPN пайдалану: Кәсіпорын жүйелеріне қашықтан қол жеткізу үшін қорғалған VPN арналарын пайдалану қажет. Бұл деректерді шифрлауды және екі факторлы аутентификацияны қамтамасыз етеді.
Құжатталған өтінім: Корпоративтік жүйелерге қол жетімділік тек ақпараттық қауіпсіздік менеджері бекіткен жазбаша өтінім негізінде беріледі.
Логирлеу: Сәтті және сәтсіз барлық қашықтан қол жеткізу әрекеттері журналдарда жазылады.

Использование внешних носителей

Рекомендации: Для передачи и хранения корпоративных данных используйте только зашифрованные внешние носители, предоставленные компанией.
Запрет на личные данные: Хранение служебной информации на личных носителях запрещено.
Удаление данных: После копирования данных на рабочую станцию, информация должна быть удалена с внешнего носителя.

Удалённый доступ

Использование VPN: Для удалённого доступа к корпоративным системам обязательно использование защищённых VPN-каналов. Это обеспечивает шифрование данных и двухфакторную аутентификацию.
Документированная заявка: Доступ к корпоративным системам предоставляется только на основании письменной заявки, утверждённой менеджером по информационной безопасности.
Логирование: Все попытки удалённого доступа, успешные и неудачные, фиксируются в журналах.