



RIIGI INFOSÜSTEEMI AMET



Краткое руководство по кибербезопасности для организаций

2025

Оглавление

1	Более устойчивые предприятия формируют более устойчивое общество.....	3
1.1	Ответственность лежит на руководителе предприятия	3
2	Определите, что именно следует защитить предприятию	5
3	Знайте, какое аппаратное и программное обеспечение вы используете	5
3.1	Проведите инвентаризацию вашего оборудования.....	6
3.2	Проведите инвентаризацию своего программного обеспечения	6
3.3	Рассмотрите возможность внедрения централизованного управления устройствами ...	7
3.4	Установите правила использования личных устройств на рабочем месте.....	7
3.5	Продумайте использование облачных сервисов	8
3.6	Безопасное использование новых технологий.....	10
4	Защитите свои ресурсы.....	12
4.1	Предоставляйте права доступа обоснованно	12
4.2	Регулярно обновляйте программное обеспечение.....	13
4.3	Обеспечьте защиту корпоративной сети и ее пользователей.....	14
4.4	Ограничьте доступ к данным на потерянных или украденных устройствах.....	14
4.5	Позаботьтесь о физической защите данных и устройств	15
5	Защитите своих сотрудников	16
5.1	Создайте политику безопасного использования паролей	16
5.2	Используйте многофакторную аутентификацию.....	17
5.3	Упростите использование паролей	17
6	Научитесь распознавать атаки	18
6.1	Повышайте осведомленность сотрудников	18
6.2	Обучайте сотрудников	19
6.3	Регулярно проверяйте знания сотрудников	19
7	Будьте готовы к инциденту и научитесь восстанавливаться	20
7.1	Знайте, как действовать в случае инцидента.....	20
7.2	Разработайте план восстановления	20
7.3	Обеспечьте контроль над тем, что происходит в системах.....	21
7.4	Обеспечьте работу системы резервного копирования и контроль за ней	21
7.5	Проводите тестовые восстановления	22
8	Защитите свой бренд.....	23
8.1	Осознайте возможные угрозы	23
8.2	Защитите себя от угроз.....	24
9	Обратите внимание на безопасность цепочки поставок	27

1 Более устойчивые предприятия формируют более устойчивое общество

Закон о кибербезопасности устанавливает требования в этой области для тех предприятий и учреждений, чья деятельность имеет жизненно важное значение – государственных органов, портов, энергетических компаний, операторов связи и других. В то же время кибербезопасность жителей Эстонии зависит еще и от того, насколько надежно все другие малые предприятия и учреждения, для которых аналогичные требования не установлены законодательно, могут защитить себя и своих клиентов (их данные). Нанять специалиста или целую команду по информационной безопасности многим не по силам, а стандарты кибербезопасности могут показаться настолько сложными и ресурсоемкими, что их внедрение не выглядит оправданным с точки зрения бизнеса.

Это краткое руководство по кибербезопасности создано для того, чтобы помочь предприятиям сделать первые шаги к более защищенным бизнес-процессам. Обеспечение информационной безопасности – это непрерывный процесс. Сделав первые шаги, имеет смысл ознакомиться с рекомендациями, приведенными в эстонском стандарте информационной безопасности для небольших организаций и предприятий.¹ Там указаны последующие меры, которые помогут ещё более эффективно выстроить информационную безопасность на вашем предприятии.

1.1 Ответственность лежит на руководителе предприятия

Начинать следует с того, что кибербезопасность – это не только задача IT-отдела. Это вопрос управления и ответственности руководства. Чем яснее руководитель понимает необходимость внедрения защитных мер, тем эффективнее он сможет направлять команду и распределять ресурсы. Руководитель играет ключевую роль в обеспечении информационной безопасности организации. Именно от его решений и действий напрямую зависит, насколько эффективно организация способна защитить свои данные и системы. Кибербезопасность – это не выбор между «всё» или «ничего». Здесь тоже можно начать с малого и постепенно двигаться вперед – так же, как предприятия регулярно пересматривают и совершенствуют свои бизнес-процессы и организацию работы.

¹ <https://eits.ria.ee/et/abimaterjalid/veits>

Что нужно делать:

1. Сделайте информационную безопасность стратегическим приоритетом предприятия и выделите на нее финансовые, технические и человеческие ресурсы.
2. Действуйте в соответствии с законами, правовыми актами и стандартами в области информационной безопасности.
3. Зафиксируйте обязанности, зоны ответственности, активы и риски организации.
4. Определите допустимый уровень рисков и назначьте ответственных за информационную безопасность.
5. Обеспечьте контроль над состоянием информационной безопасности и инцидентами, которые могут возникнуть.
6. Регулярно проводите обучение по безопасности и вкладывайтесь в повышение осведомленности сотрудников.
7. Формируйте рабочую среду, в которой ценится информационная безопасность. Подавайте личный пример, следуя лучшим практикам и внутренней политике в сфере безопасности.

2 Определите, что именно следует защитить предприятию

Информационная безопасность начинается с четкого понимания: что мы защищаем и зачем. Часто именно (малые и средние) предприятия могут быть не в состоянии понять важность кибербезопасности и риски, связанные с недостаточной информационной безопасностью.

Потребность в защите – это совокупность требований безопасности, которые необходимо соблюдать для надежного функционирования бизнес-процессов организации. Чтобы оценить потребность в защите, стоит продумать различные сценарии ущерба, например:

1. Какие нормативные акты и договоры накладывают на организацию требования и ожидания?
2. Какие последствия может повлечь деятельность организации для жизни и здоровья людей?
3. Какие убытки возможны, если задачи организации не будут выполнены или качество работы окажется ниже ожидаемого уровня?
4. Какие последствия может вызвать ущерб, нанесенный репутации организации?
5. К каким финансовым потерям могут привести сбои в работе данных и систем?

Анализ таких сценариев помогает организации выявить наиболее уязвимые области, в защиту которых необходимо в первую очередь вкладываться. Кроме того, это позволяет определить допустимый уровень риска – в каких случаях достаточно просто следить за ситуацией, а в каких требуется немедленно применять защитные меры.

В цифровом обществе очень важно, чтобы безопасность стала неотъемлемой частью работы предприятия, а управление рисками безопасности рассматривалось как элемент общего управления бизнес-рисками. Когда предприятие четко определило свои потребности в защите, реализация мер безопасности получает конкретную и осмысленную цель. Кроме того, такая оценка служит ориентиром в ситуациях, когда истекает срок действия договора, меняется законодательство или происходит смена подрядчика – чтобы сразу было понятно, какие аспекты в управлении безопасностью требуют пересмотра.

3 Знайте, какое аппаратное и программное обеспечение вы используете

Чтобы эффективно защитить сеть предприятия, нужно в первую очередь четко понимать, какие устройства и программы в ней задействованы. Именно поэтому инвентаризация – это первый и крайне важный шаг на пути к созданию защищенной системы. Если нет ясности, какое оборудование и программное обеспечение должно быть в сети, невозможно будет заметить, когда в нее попадут неизвестные или несанкционированные элементы. Именно такие устройства и программы могут использовать злоумышленники, чтобы проникнуть в корпоративную сеть. Если не известно, какое программное обеспечение установлено, его не удастся вовремя обновить. Кроме того, может оказаться, что установлено программное обеспечение, через которое в систему может попасть вредоносный код – например, нелегальные

программы для загрузки музыки или фильмов. Для каждого устройства в сети предприятия необходимо знать следующую информацию:

1. идентификатор или название устройства;
2. производитель и модель;
3. серийный номер устройства.
4. IP-адрес;
5. назначение устройства – зачем оно подключено к сети (например, рабочий компьютер, сервер, сетевое оборудование и т. п.);
6. список установленного на устройстве программного обеспечения;
7. какие бизнес-процессы зависят от работы этого устройства;
8. как это устройство связано с другими ресурсами предприятия.

3.1 Проведите инвентаризацию вашего оборудования

Прежде всего, необходимо установить, какие именно устройства находятся в сети. Даже если речь идет о небольшой сети с парой компьютеров, эти данные обязательно нужно задокументировать. Если этого не сделать, устройства могут остаться без защиты. Как раз незащищенные устройства чаще всего становятся входной точкой для атак на сеть предприятия. Обзор устройств в сети также необходим, когда происходит смена IT-специалистов или поставщиков услуги, потому что им нужна информация о сети и устройствах в ней.

Если сеть предприятия состоит не из пары компьютеров, а из большего числа устройств, имеет смысл использовать специальное программное обеспечение, которое проводит инвентаризацию автоматически. Ручной сбор данных чреват ошибками, а при большом количестве оборудования занимает слишком много времени. В реестр оборудования нужно включать не только те устройства, которые подключены к сети в данный момент, но и те, что могут быть подключены в будущем или содержат данные, потеря которых может повлечь за собой серьезные последствия – например, в случае кражи.

3.2 Проведите инвентаризацию своего программного обеспечения

После того как составлен список всех устройств в сети, следующим шагом будет определить, какое программное обеспечение установлено на каждом из них. Это необходимо для того, чтобы убедиться, что все программы обновлены и что на устройствах не установлено лишнего или ненадежного софта, не связанного с рабочими задачами. Как и в случае с оборудованием, для инвентаризации программ лучше всего использовать инструменты, которые собирают данные автоматически. Автоматизированные решения позволяют не только сократить время, но и вовремя замечать появление нового ПО на устройствах. Собранные сведения о программах должны быть связаны с реестром оборудования, чтобы отслеживать все устройства и установленный на них софт из одного места.

Посоветуйтесь с IT-специалистом

Для инвентаризации оборудования и программного обеспечения можно использовать как бесплатные, так и платные инструменты. Платные решения, как правило, предлагают больше возможностей и гибкости. Узнайте у IT-специалистов вашей организации или поставщика услуг о соответствующем программном обеспечении.

3.3 Рассмотрите возможность внедрения централизованного управления устройствами

Чтобы упростить администрирование устройств и программного обеспечения, имеет смысл рассмотреть внедрение централизованной системы управления. Централизованное управление позволяет контролировать устройства через единую систему, определять, какое программное обеспечение должно быть установлено, и отказаться от множества отдельных решений для учета и управления. Такая система позволяет не только вести учет оборудования, но и автоматически применять к устройствам требования по информационной безопасности. Некоторые системы централизованного управления позволяют удаленно стереть данные с устройства через интернет. Это особенно полезно, если устройство будет утеряно или украдено.

Посоветуйтесь с IT-специалистом

Существует несколько решений для централизованного управления, в зависимости от того, какие устройства (компьютеры, интеллектуальные устройства) используются. Обычно они являются платными. Узнайте у своих IT-специалистов или поставщика услуг подходящие для вашего предприятия решения.

3.4 Установите правила использования личных устройств на рабочем месте

Сегодня всё чаще сотрудники хотят использовать для работы личные устройства. Особенно распространены смартфоны и планшеты, но всё чаще применяются и личные ноутбуки. Кроме того, сотрудники приносят на работу свои USB-накопители и внешние жесткие диски, с помощью которых можно быстро и просто перенести данные из внутренней сети на внешний носитель.

Если сотрудникам разрешено использовать личные устройства, необходимо установить четкие правила, поскольку на таких устройствах обрабатываются данные предприятия. По возможности такие правила стоит разрабатывать совместно с пользователями и IT-специалистами.

При составлении правил использования личных устройств необходимо:

1. определить, какие требования безопасности распространяются на такие устройства. Например, обязательно нужно требовать, чтобы устройство было защищено паролем и на нем было установлено антивирусное программное обеспечение;

2. составить список устройств и операционных систем, которые нельзя использовать в организации – например, устройств с известными уязвимостями или тех, чья операционная система больше не поддерживается производителем. В организации должно быть запрещено использование личных сетевых устройств – таких как собственные коммутаторы (*switch*), роутеры, Wi-Fi-устройства и тому подобное, поскольку они могут нарушить работу корпоративной сети;
3. по возможности ведите список личных устройств, которые сотрудники хотят использовать. В нем стоит указывать имя сотрудника, название устройства, список установленного программного обеспечения и другую важную информацию.
4. разработать инструкции по использованию внешних носителей, таких как USB-накопители или внешние жесткие диски;
5. При необходимости установите правило, запрещающее хранить рабочую информацию на личных устройствах.

Сотрудники должны быть ознакомлены с принятыми правилами и требованиями, согласиться с ними и подтвердить это своей подписью. Без этого использовать личное устройство для работы не допускается.

3.5 Продумайте использование облачных сервисов

Облачные технологии предоставляют предприятиям широкие возможности: гибкость, экономию затрат и более удобный доступ к данным. Однако вместе с этими преимуществами они несут и новые риски, которые нужно осознанно контролировать. Ниже приведены ключевые принципы, которые помогут принимать взвешенные решения при выборе и использовании облачных решений, обеспечивая при этом безопасность данных предприятия.

3.5.1 Выберите подходящего поставщика услуг

В первую очередь важно правильно выбрать поставщика облачных сервисов. Это стратегическое решение, напрямую влияющее на безопасность данных. Тщательное планирование и осознанный выбор позволяют получить максимум пользы от облачных технологий и одновременно минимизировать возможные риски. Основные аспекты, на которые стоит обратить внимание при выборе поставщика облачных услуг:

1. Убедитесь, что поставщик соблюдает соответствующие стандарты безопасности и нормативные требования.
2. Важно знать, где хранятся данные и как осуществляется их обработка – это критично как с точки зрения защиты данных, так и с точки зрения соответствия требованиям законодательства.
3. Оцените надежность и доступность сервиса – полезной будет информация о предыдущих инцидентах и о том, как поставщик их решал;
4. Качественная служба поддержки имеет решающее значение. Стоит убедиться, что облачная платформа предоставляет своевременную и профессиональную помощь.

5. Ознакомьтесь с условиями договора и стоимостью услуг. Важно обращать внимание на то, чтобы использование сервиса не сопровождалось скрытыми платежами или договорными обязательствами, особенно при передаче данных в случае прекращения обслуживания.

Перед тем как принять решение, стоит изучить предложения нескольких поставщиков, сравнить условия и ознакомиться с отзывами клиентов.

3.5.2 Безопасное использование облачных сервисов

После того как подходящий поставщик выбран, необходимо сосредоточиться на безопасной настройке и эксплуатации облачной платформы. Уже на этапе внедрения следует продумать все параметры безопасности – например, контроль доступа, настройки сетевой безопасности и ведение логов. Многие облачные сервисы предоставляют встроенные функции защиты, которые помогают бороться с киберугрозами – фильтрация спама или вредоносного контента. Периодически проверяйте имеющиеся функции безопасности и, если потребуется, в панели управления включите дополнительные меры, установив их как обязательные для каждого пользователя. Настроить платформу правильно – это только первый шаг. Но чтобы всё работало безопасно и надежно в будущем, нужно думать не только о настройке, но и о постоянной защите. Чтобы защитить систему и не дать злоумышленникам воспользоваться известными уязвимостями, облачные сервисы нужно регулярно обслуживать и обновлять. Не менее важно вести системное логирование и постоянный мониторинг – это позволяет быстро заметить подозрительную активность. Чтобы эффективно выявлять и реагировать на потенциальные инциденты в облачной среде, необходимо настроить систему сбора журналов событий и осуществлять постоянный мониторинг происходящего.

Не стоит также забывать о создании резервных копий данных. Наличие облачного хранилища не освобождает от необходимости регулярного создания резервных копий – наоборот, это делает его еще более актуальным. Необходимо регулярно создавать резервные копии и убедиться, что они хранятся в защищенном виде. Некоторые сервисы предоставляют встроенные функции резервного копирования, но как минимум одна копия всегда должна храниться отдельно – либо на физическом носителе под контролем организации, либо в другом облачном сервисе. Это обеспечит возможность восстановления данных в случае непредвиденных сбоев. Подробнее о безопасном резервном копировании можно прочитать в разделе 7.3 «Обеспечьте работу системы резервного копирования и контроль за ней».

3.5.3 Знайте, кто имеет доступ к облачным сервисам

Внутри предприятия необходимо тщательно продумать, кто и к каким ресурсам имеет доступ. Каждый сотрудник должен получать лишь тот уровень доступа, который необходим для выполнения его служебных обязанностей – не больше.

В облачных сервисах для каждого пользователя создается индивидуальная учетная запись, управление которой осуществляется самой организацией. Каждая учетная запись должна быть защищена надежным и уникальным паролем, а также многофакторной аутентификацией. Также важно не забывать своевременно закрывать

доступ сотрудников, покидающих организацию – соответствующие учетные записи необходимо деактивировать не позже последнего рабочего дня, чтобы бывшие сотрудники не сохранили доступ к данным предприятия. Это позволяет избежать ситуаций, когда неавторизованные лица получают доступ к конфиденциальной информации. Больше информации о том, как предоставить права доступа и защитить учетные записи, можно найти в разделе 4.1 «Предоставляйте права доступа обоснованно» и в разделе 5 «Защите своих сотрудников».

Учетная запись администратора обладает более широкими правами, чем обычная. Поэтому администрированием облачных сервисов следует заниматься с использованием отдельной учетной записи администратора, которая не применяется для повседневной работы. При использовании облачных платформ очень важно, чтобы у организации всегда сохранялся доступ с правами администратора к своей пользовательской среде (то есть к обособленному и изолированному облачному пространству, предназначенному конкретно для этой организации). На этапе создания такой среды необходимо заранее выяснить, как у выбранного поставщика облачных услуг можно восстановить доступ администратора в экстренной ситуации, и настроить соответствующие параметры. Например, может потребоваться указать резервные контактные данные администратора (например, дополнительный адрес электронной почты) и сохранить коды восстановления в безопасном месте вне облачной среды – например, в физическом сейфе. Учетные записи администраторов также должны быть защищены надежными паролями и многофакторной аутентификацией. Некоторые облачные сервисы позволяют ограничивать доступ к пользовательской среде или панели управления, разрешая его только с определенных IP-адресов или устройств. Стоит также рассмотреть возможность использования условных правил доступа (*Conditional Access Policies*) – они позволяют гибко задавать, кто и при каких условиях может получить доступ к сервисам: в зависимости от местоположения, уровня безопасности устройства, времени суток или используемого приложения. Такие механизмы обеспечивают более гибкую и надежную защиту по сравнению с обычными статичными правилами.

Важно предоставить сотрудникам четкие инструкции по использованию облачных сервисов и познакомить их с возможными рисками, связанными с платформой. Осведомленный и подготовленный персонал может предотвратить множество распространенных угроз, которые зачастую возникают из-за недостатка внимания или недостаточных знаний.

3.6 Безопасное использование новых технологий

Искусственный интеллект (ИИ) и машинное обучение могут помочь предприятию развиваться, ускорять процессы и снижать издержки. При этом важно понимать, что новые технологии также несут в себе риски.

Полезно знать!

Департамент государственной инфосистемы (RIA) и компания Cybernetica AS изучили риски, связанные с технологиями ИИ, а также возможные меры по их снижению в малых и средних предприятиях. Подробнее об этом можно прочитать здесь: <https://www.ria.ee/sites/default/files/documents/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf>.

Чтобы предприятие могло использовать искусственный интеллект грамотно, ответственно и безопасно, необходимо заранее продумать шаги по управлению сопутствующими рисками.

1. Продумайте, зачем и для чего вы используете ИИ

Прежде чем внедрять искусственный интеллект, важно четко понимать, какую задачу он должен решать, какие данные он будет использовать и как устроена его техническая архитектура. Четкое описание системы – это основа для понимания возможных рисков.

2. Разберитесь во всем жизненном цикле

ИИ-система – это не просто «технология, которую включили». У нее есть этапы: запуск, разработка, эксплуатация и последующее сопровождение. Поэтому нужно зафиксировать весь жизненный цикл – от планирования и сбора данных до внедрения и постоянного отслеживания. Риски могут возникнуть на любом этапе, поэтому нужно всё время быть в курсе и постоянно контролировать процесс. Также важно определить, кто за что отвечает на каждом этапе и что может пойти не так.

3. Убедитесь, что всё соответствует закону

Если ИИ использует персональные данные (например, информацию о клиентах), необходимо соблюдать требования законодательства о защите данных, такие как GDPR, а также учитывать специфические отраслевые нормы. Проверьте, соответствует ли ваша деятельность законодательству, и есть ли у вас все необходимые разрешения и согласия.

4. Оцените, на кого это повлияет

Кроме технических и правовых аспектов, важно учитывать и более широкий социальный контекст. ИИ может повлиять на клиентов, сотрудников, местное сообщество или даже окружающую среду. Задайтесь вопросом: может ли система быть несправедливой, отдавать предпочтение одной группе перед другой или вызвать путаницу и беспокойство? Подобные риски могут быть неочевидными на первом этапе, но в долгосрочной перспективе привести к серьезным последствиям.

5. Оценивайте риски и находите решения

После того как риски выявлены, важно подобрать подходящие меры для их снижения. Составьте перечень возможных проблем и оцените, насколько серьезными они могут быть. Затем выберите соответствующие меры – возможно, потребуется усилить информационную безопасность, уточнить внутренние правила или провести дополнительное обучение сотрудников. Взвешенный подход к управлению рисками помогает предотвратить проблемы и повышает доверие пользователей.

4 Защитите свои ресурсы

Когда у вас есть четкое представление о том, какие устройства и программы используются в офисной сети и находятся в распоряжении сотрудников, следующий шаг – защита этих ресурсов.

Поскольку устройства и сервисы (например, веб-сайт, бизнес-приложения и т. п.) могут размещаться у внешнего поставщика или уже иметь какую-либо встроенную защиту (файрвол, антивирус), может показаться, что используемые в предприятии оборудование и программное обеспечение уже достаточно защищены. Однако этого недостаточно для реальной защиты от угроз. Чтобы эффективно защитить устройства и данные, необходимо применять дополнительные меры и относиться к этому как к постоянному процессу, а не одноразовой задаче.

4.1 Предоставляйте права доступа обоснованно

Атаки и вирусы чаще всего проникают в систему через пользователей. Чем больше у пользователя прав, тем легче злоумышленнику или вредоносному ПО действовать от его имени.

Именно поэтому каждое предоставление доступа – будь то к общей папке, бухгалтерской системе или администраторские права на компьютере – должно быть тщательно обдумано. Нужно честно ответить на вопрос: действительно ли эти права необходимы для выполнения рабочих задач? Если да, то следует руководствоваться принципом минимальных привилегий: работник должен получить только те права, которые строго необходимы для работы, и ни каплей больше. Часто, чтобы сэкономить время, предоставляют доступ ко всему каталогу – в результате сотрудник может получить доступ к данным, к которым он не должен иметь доступа. Даже если он сам ими не воспользуется, этим могут воспользоваться злоумышленники.

Добросовестная практика!

Выдавайте права доступа через группы. Это упростит управление доступом и даст более полную картину, кто к чему имеет доступ. Если сотрудник уходит, его можно просто удалить из группы, не просматривая вручную десятки каталогов и не гадая, к чему он имел доступ.

В повседневной работе следует использовать учетную запись с правами обычного пользователя, а не администратора. Права администратора несут в себе серьезные риски:

1. сотрудник может установить программы, которые откроют уязвимости или приведут к заражению системы;
2. вредоносное ПО нанесет куда больший ущерб, если запущено с правами администратора;
3. злоумышленникам будет гораздо проще получить полный контроль над компьютером.

Если права администратора всё же необходимы, то для этого пользователя следует создать отдельную учетную запись с соответствующими правами, которую нужно использовать только при необходимости, а не для повседневной работы. Правильно организованная система резервного копирования существенно снижает риск потери данных – даже если вредоносное ПО будет установлено случайно или утекут учетные данные сотрудника, злоумышленник не получит немедленного доступа к критически важным ресурсам. Если это персональный компьютер сотрудника, то надо следовать пункту 3.4 «Создайте правила использования личных устройств в рабочей среде», но в этом случае также следует рекомендовать отдельную учетную запись для рабочей информации.

Посоветуйтесь с IT-специалистом

Обратитесь к своему IT-специалисту или поставщику услуг с просьбой о регулярном обзоре используемых учетных записей администратора.

Если IT-специалист или поставщик услуг предоставляет права доступа, то они также должны документировать эти разрешения (когда, для чего, кому), чтобы иметь актуальный обзор того, кто имеет доступ. Эта информация также полезна, когда сотрудник уходит, поскольку тогда известно, какие права должны быть закрыты. Необходимо также помнить о том, что доступ сотрудников, покинувших организацию, должен быть своевременно закрыт, а все их права – удалены.

4.2 Регулярно обновляйте программное обеспечение

Использование программного обеспечения – неотъемлемая часть современной работы. Однако в любом программном обеспечении со временем обнаруживаются уязвимости и другие недостатки, которыми злоумышленники могут воспользоваться, чтобы установить вредоносный код, получить контроль над устройством или похитить данные. Именно поэтому регулярное обновление программного обеспечения – одна из важнейших и одновременно самых простых мер по защите ресурсов предприятия.

Если программа поддерживает автоматическое обновление (например, операционные системы на компьютерах и мобильных устройствах), этот функционал обязательно нужно включить. Если автоматическое обновление не предусмотрено (например, в случае отдельных программ или прошивок сетевого оборудования), его нужно выполнять вручную – самостоятельно, через IT-специалиста или с помощью подрядчика. Альтернативный вариант – использовать решения, которые позволяют автоматизировать обновление. Многие современные антивирусные решения предлагают функции, позволяющие удобно и автоматически обновлять программное обеспечение.

Если производитель больше не поддерживает используемую версию ПО или оборудования, нужно перейти на поддерживаемую версию или заменить оборудование. Например, с 2025 года Microsoft прекращает поддержку компьютеров с операционной системой Windows 10. В такой ситуации следует перейти на самую актуальную версию Windows или рассмотреть возможность перехода на альтернативную операционную систему. Использование устаревшего ПО может негативно сказаться на безопасности

устройства, его совместимости и получении технической поддержки, что влечет за собой различные риски. В частности, новые уязвимости и сбои в старом ПО могут оставаться без исправлений. Это делает систему более уязвимой для атак со стороны киберпреступников. Даже если на данный момент в устаревшей системе еще не обнаружены критические уязвимости, это лишь вопрос времени, когда они будут найдены и использованы. Нужно исходить из простого принципа: если есть уязвимость – найдется и тот, кто ее использует. Грамотное управление ресурсами предприятия помогает отслеживать необходимость и факт установки обновлений.

4.3 Обеспечьте защиту корпоративной сети и ее пользователей

Граница между корпоративной сетью и публичным интернетом называется периметром. Чем меньше подозрительного трафика проникает в сеть предприятия, тем ниже риск для сотрудников и устройств, работающих внутри этой сети. Главный инструмент защиты периметра – это межсетевой экран (другие названия – файрвол, брандмауэр). Он действует как посредник между интернетом и корпоративной сетью и фильтрует потенциально опасный трафик. Современные файрволы с расширенными функциями не только блокируют вредоносные соединения, но и могут выявлять попытки атак на сеть предприятия и эффективно их останавливать. Кроме того, они позволяют управлять тем, какие сайты доступны сотрудникам. Например, можно запретить доступ к заведомо вредоносным или сомнительным ресурсам, откуда может загружаться вредоносное ПО. Файрвол также позволяет контролировать, какие приложения, используемые сотрудниками, имеют доступ в интернет. Например, можно заблокировать программы для загрузки фильмов или музыки с нелегальных источников.

Поскольку значительная часть вирусов и атак распространяется через электронную почту, на почтовом сервере обязательно должно быть установлено антивирусное и антиспам-программное обеспечение. Такое программное обеспечение автоматически отсекает подозрительные письма (спам, фишинг, вирусы и прочее) до того, как они попадут в почтовые ящики сотрудников. Большинство почтовых серверов имеют базовую встроенную защиту от спама. Антиспам-фильтры могут быть реализованы в виде облачного сервиса или хостингового решения (то есть вне сети предприятия), либо как отдельный сервер внутри корпоративной сети. Более продвинутые решения включают в себя полезные функции, которые упрощают работу сотрудников: автоматическая рассылка отчетов о заблокированных письмах, возможность вручную освободить нужное письмо, заблокировать отправителя и многое другое.

Однако злоумышленники изобретательны, и вредоносные письма все равно периодически попадают к пользователям. Именно поэтому на всех устройствах обязательно должно быть установлено антивирусное программное обеспечение. Важно следить, чтобы антивирус всегда был актуален: использовалась последняя версия, обновления устанавливались вовремя, а все защитные функции были включены. Только при этих условиях антивирус способен эффективно выполнять свою задачу.

4.4 Ограничьте доступ к данным на потерянных или украденных устройствах

И всё же рано или поздно может случиться, что сотрудники потеряют свои устройства – смартфоны, планшеты, ноутбуки и т. д. – или эти устройства попадут в руки злоумышленников. Поскольку на них могут храниться конфиденциальные данные

предприятия или другая чувствительная информация, крайне важно заранее продумать, что делать в подобных ситуациях.

Одно из решений описано в разделе 3.3 «Рассмотрите возможность внедрения централизованного управления устройствами». Такая система позволяет при утере устройства удаленно его заблокировать, определить его местоположение или полностью стереть с него все данные. Для мобильных устройств, таких как телефоны и планшеты, существуют бесплатные приложения с аналогичным функционалом – их стоит внедрить заранее.

Ограничить доступ к данным также помогает шифрование. Если компьютер или внешний жесткий диск будет украден или утерян, никто не сможет прочитать содержащиеся на нем данные без правильного пароля или ключа. Шифрование делает информацию нечитаемой для посторонних, и это особенно важно, если на устройстве хранится конфиденциальная информация – например, финансовые данные, персональные сведения или коммерческая тайна. Современные компьютеры уже оснащены встроенными средствами шифрования, такими как BitLocker или FileVault. Существуют и другие программы для шифрования, которые могут обеспечить дополнительный уровень защиты. При этом важно помнить: шифрование будет эффективно только в том случае, если используется надежный пароль и он хранится в безопасном месте.

4.5 Позаботьтесь о физической защите данных и устройств

Помимо программных средств защиты, необходимо уделить внимание и физической безопасности оборудования. Все устройства, на которых хранятся важные данные, должны быть защищены от доступа посторонних. Нет смысла в мощном межсетевом экране, если в офис может спокойно зайти посторонний, пройти в серверную и получить физический доступ к устройствам.

Серверы, сетевое оборудование и другие критически важные устройства должны находиться в отдельных шкафах или в специально предназначенном серверном помещении. Шкаф или дверь в серверную должны быть заперты, а ключ – храниться в надежном месте. Также следует вести журнал посещений серверной: кто, когда и с какой целью туда заходил. Это поможет в случае необходимости установить, кто имел доступ к оборудованию.

Посоветуйтесь с IT-специалистом

Если сервер размещен у внешнего провайдера, убедитесь, что у него есть учет того, кто имеет физический доступ к серверу и кто фактически им пользовался.

Чтобы сервер работал стабильно, его нужно обеспечить надлежащим охлаждением (например, кондиционером в серверной) и подключением к источнику бесперебойного питания (UPS), чтобы защитить от перебоев в электроснабжении. Иначе в жаркий день сервер может просто отключиться, а при резком отключении электроэнергии – данные повредиться.

Если в офисе есть неиспользуемые сетевые розетки, нужно убедиться, что через них невозможно получить доступ к сети. Попросите IT-специалиста или обслуживающую компанию отключить их или правильно настроить. Иначе может возникнуть ситуация,

когда кто угодно подключит к розетке свой компьютер и получит доступ ко всем корпоративным устройствам. Следующий шаг – логически разделить сеть на сегменты, чтобы компьютеры и серверы находились в разных зонах. Тогда даже если кто-то получит доступ к рабочей сети, он не сможет сразу попасть на серверы. Для сотрудников и гостей необходимо создавать отдельные Wi-Fi-сети – это предотвращает доступ посторонних лиц к внутренней корпоративной сети.

Не менее важно обучать сотрудников не оставлять рабочие устройства без присмотра и не забывать их в общественных местах, всегда блокировать экран, отходя от компьютера и никогда не передавать свои устройства посторонним.

5 Защитите своих сотрудников

Для защиты данных и пользователей крайне важно, чтобы доступ к любой системе был возможен только после ввода пароля или с помощью другого метода аутентификации. Пароль должен быть достаточно сложным, чтобы его было трудно угадать. Если система не защищена паролем или используется простой, легко предсказуемый пароль, вредоносное ПО и злоумышленники смогут значительно проще получить к ней доступ. Это может привести к утечке данных, их уничтожению или даже подмене важной информации.

5.1 Создайте политику безопасного использования паролей

Аутентификация – это процесс, с помощью которого система проверяет, действительно ли человек, пытающийся войти, является тем, за кого себя выдает. На практике чаще всего для этого применяются пароли или цифровые сертификаты.

Чтобы корпоративная сеть была надежно защищена, необходимо установить правила по сложности и длине паролей. Если есть подозрение, что пароль стал известен третьим лицам, или произошел инцидент безопасности – пароль нужно сменить немедленно. Для всех аккаунтов – рабочих, личных, а также учетных записей в социальных сетях – следует использовать разные пароли. Надежный пароль должен быть длинным (не менее 15 символов), содержать специальные символы и быть уникальным. Вместо обычного пароля рекомендуется использовать пароль-фразу. Контрольная фраза состоит из четырех-пяти слов, составляющих предложение (например: Koshk@Murknu1a2raz@) – оно длиннее, но проще для запоминания, чем пароль со случайными символами. В пароле желательно использовать прописные и строчные буквы, символы (точка, запятая, восклицательный знак и т. д.) между словами. Пароль должен легко запоминаться, но при этом не должен слишком легко угадываться.

Если настройки системы позволяют, то все предложенные выше параметры должны устанавливаться автоматически, так как пользователь всегда выбирает самый простой путь для создания пароля. Если системная настройка невозможна, то пароли необходимо регулярно менять вручную и постоянно напоминать об этом пользователям. Небольшие предприятия обычно не имеют отдельной политики паролей, однако важно, чтобы пароли использовались в соответствии с надлежащей практикой безопасности.

Посоветуйтесь с IT-специалистом

Уточните у вашего IT-специалиста или поставщика услуг, отвечает ли текущая политика паролей современным стандартам защиты. При необходимости следует разработать и внедрить политику управления паролями.

5.2 Используйте многофакторную аутентификацию

С ростом популярности облачных сервисов всё больше корпоративных ресурсов становятся доступны в интернете из любой точки мира. А если сервис доступен публично, он становится и более уязвимым для атак. Если используемый вами облачный сервис (например, Office 365, Gmail, Dropbox и другие) поддерживает многофакторную аутентификацию, ее обязательно нужно включить. Это означает, что помимо пароля требуется дополнительный способ аутентификации – например, ввод кода, подтверждение на телефоне, использование ID-карты, криптотокена или аппаратного устройства, такого как YubiKey.

Если включена многофакторная аутентификация, злоумышленники не смогут получить доступ к системе даже при утечке пароля, поскольку у них не будет второго компонента, необходимого для подтверждения личности.

5.3 Упростите использование паролей

Поскольку большинство систем требует ввода пароля, у сотрудников часто накапливается множество разных логинов и паролей. В результате они начинают записывать их на бумаге, использовать один и тот же пароль в разных системах или придумывать слишком простые комбинации. Чтобы избежать таких рисков, имеет смысл внедрить менеджер паролей – специальное программное обеспечение, которое позволяет надежно хранить и использовать пароли. Существует множество таких решений, включая бесплатные варианты.

Если в организации используется большое количество устройств, стоит рассмотреть возможность внедрения централизованной системы управления пользователями. В среде Microsoft Windows таким решением является, например, Active Directory (AD). Active Directory (AD) – это сервис, который обеспечивает интегрированную аутентификацию в среде Windows. С его помощью пользователи могут входить во все устройства, подключенные к домену, используя один и тот же логин и пароль. До внедрения домена для каждой из этих систем могли быть отдельные пароли. С переходом на домен достаточно одного – это удобно и безопаснее. Использование AD-домена требует наличия Windows-сервера. Существуют и облачные альтернативы, не требующие собственного сервера, например, Azure AD, который работает в связке с лицензиями Office 365. Некоторое бизнес-программное обеспечение также можно интегрировать с AD-доменом или Azure AD. Централизованное управление пользователями позволяет, среди прочего, быстро отключить доступ ушедшему сотруднику – все делается из одного интерфейса.

6 Научитесь распознавать атаки

Любая система настолько надежна, насколько прочна ее самая слабая часть. И чаще всего именно пользователь оказывается этой слабой точкой. Злоумышленники прекрасно это понимают и стараются получить доступ к системам именно через сотрудников – рассылая письма с вирусами или фишинговыми ссылками, чтобы выманить пароли, банковские данные или даже деньги. Кроме того, в интернете полно сайтов, цель которых – обмануть пользователя, заразить устройство или похитить информацию. Поэтому крайне важно обучать сотрудников, как распознавать угрозы и правильно действовать при столкновении с ними. Информирование и обучение персонала – один из ключевых шагов в обеспечении безопасности предприятия.

6.1 Повышайте осведомленность сотрудников

За последние годы киберпреступники стали гораздо изощреннее, и отличить мошенническое письмо или вредоносный сайт от настоящих становится все труднее.

Сотрудникам необходимо объяснять, какие типы атак встречаются чаще всего, как их распознать и как правильно действовать в случае подозрений. Проводить такие инструктажи может IT-отдел или -внешний подрядчик.

Если какое-либо электронное письмо, которое вы получаете, кажется подозрительным, всегда стоит обратиться к IT-персоналу своей организации или поставщику услуг, чтобы они просмотрели это письмо. Даже если окажется, что письмо было безопасным, лучше лишний раз проверить, чем потом сожалеть.

Сотрудники должны быть обучены распознавать мошеннические и фишинговые электронные письма и опасные веб-сайты:

1. Следует внимательно проверять адрес отправителя: даже если он кажется настоящим, обычно в нем есть небольшие изменения. Например, вместо «@eesti.ee» может быть «@eetsi.ee». Иногда адрес в строке «От» выглядит нормально, но если нажать «Ответить», становится видно, что письмо уйдет совсем другому получателю.
2. В случае с веб-сайтами следует смотреть на их адрес. Как и в случае с адресами электронной почты, в них могут быть изменения: например, вместо «.ee» в конце будет «.ea» или буквы в адресе заменены цифрами – например, вместо «eesti.ee» будет «eest1.ee».
3. Будьте особенно насторожены, если письмо или сайт обещает деньги, приз, бесплатную поездку, ценные подарки и т. п. – это почти всегда обман.
4. Если письмо пришло якобы от имени руководства или бухгалтерии, стоит обратить внимание, соответствует ли стиль письма привычной манере общения, особенно если в нем содержится просьба о денежном переводе. Мошеннические электронные письма обычно подозрительно короткие и носят угрожающий тон (например, в стиле «Оплатите немедленно, это должно быть оплачено в течение 24 часов! и т. д.).

6.2 Обучайте сотрудников

В дополнение к общему повышению уровня кибербезопасности в организации следует проводить обучение сотрудников по вопросам киберугроз и цифровой гигиены. Такое обучение должно охватывать более широкий круг тем, связанных с безопасностью: поведение в социальных сетях, использование публичных облачных сервисов, правила безопасной работы с Wi-Fi и т. п.

Программа обучения может включать:

1. ознакомление с внутренними правилами информационной безопасности предприятия, объяснение требований и возможных рисков;
2. анализ угроз, связанных с различными устройствами и сервисами (переносные устройства, соцсети, публичные облачные платформы и др.);
3. инструкции по действиям при инцидентах безопасности (кого уведомить, что предпринять и т. д.);
4. обучение распознаванию потенциальных угроз и наиболее распространенных способов атак, а также оценку возможных последствий таких атак;
5. разбор недавних инцидентов, получивших огласку, с объяснением причин и возможных способов их предотвращения. Один из вариантов – участие в программе «Кибертест», предлагаемой RIA. Кибертест – это онлайн-платформа для обучения, цель которой – повысить и поддерживать уровень киберосведомленности сотрудников учреждений и предприятий. Содержимое Кибертеста обновляется ежегодно. Больше информации о программе вы найдете на [сайте](#) RIA²:

6.3 Регулярно проверяйте знания сотрудников

Чтобы понять, насколько эффективно общее обучение и инструктаж по вопросам кибербезопасности, необходимо регулярно проверять уровень знаний сотрудников. Это помогает освежить в памяти полученные знания и закрепить их. Проверку можно проводить, например, с помощью опросов, которые предлагают компании, специализирующиеся на услугах и обучении в сфере кибербезопасности – именно они лучше всего умеют актуализировать такие тесты. Таким образом предприятие может выяснить, требуется ли повторное обучение по каким-либо темам.

Для оценки поведения сотрудников полезно также проводить небольшие практические проверки – например, разослать им поддельное фишинговое письмо. Результаты таких тестов подскажут вам, что еще нужно рассказать пользователям или нужно ли дополнительное обучение. Сообщайте сотрудникам о результатах анализа инцидентов и привлекайте их к разработке правил. Так они будут более мотивированы соблюдать эти правила. Проверку знаний сотрудников можно проводить с помощью Кибертеста, о котором говорилось в пункте 6.2 «Обучайте сотрудников».

² <https://www.ria.ee/kuberturvalisus/kuberruumi-analuus-ja-ennetus/kubertest>

7 Будьте готовы к инциденту и научитесь восстанавливаться

Время от времени могут возникать ситуации, при которых данные (файлы, электронная почта, базы данных и т. п.) удаляются или повреждаются. Причиной может быть, например, случайное удаление файла сотрудником или его перезапись с ошибочными данными. Кроме того, существуют кибератаки, кражи оборудования или несчастные случаи (пожары, затопления), которые могут полностью уничтожить или повредить данные. Именно поэтому предприятию необходим четкий план действий на случай инцидента, а также надежная система резервного копирования с хранением копий в защищенном месте.

7.1 Знайте, как действовать в случае инцидента

О факте киберинцидента нужно сообщить в отдел реагирования на инциденты RIA – CERT-EE: cert@cert.ee. Для консультаций и анализа важно, чтобы организация была готова делиться подробностями инцидента и назначила контактное лицо, уполномоченное на общение с CERT-EE.

В случае инцидента начните с фиксации ситуации:

1. сохраните логи как с локальных систем, так и с лог-серверов;
2. зафиксируйте текущую конфигурацию (например, правила файрвола);
3. сделайте образы дисков с затронутых систем;
4. Сохраните хотя бы последнюю резервную копию до момента инцидента, а если возможно, то все резервные копии, относящиеся к затронутым системам.

После того как ситуация зафиксирована, следует определить масштаб инцидента и перечислить все затронутые системы. Системы, которые были скомпрометированы или могут быть скомпрометированы, необходимо как можно быстрее изолировать.

При восстановлении IT-сервисов важно не уничтожить логи и другие важные доказательства, которые могут понадобиться для расследования. По итогам анализа первопричин инцидента следует запланировать действия, которые помогут в будущем избежать аналогичной ситуации.

Если киберинцидент затронул клиентов или партнеров, их нужно своевременно уведомить. В ряде случаев, например при утечке персональных данных, предприятие обязано уведомить Инспекцию по защите данных. Также стоит заранее оценить, нужно ли составить официальный отчет о произошедшем и направить его в полицию.

7.2 Разработайте план восстановления

Для обеспечения непрерывности работы предприятия важно создать план восстановления. Даже если кажется, что в случае сбоя всё и так понятно, как восстановить систему, по законам Мерфи можно с большой долей уверенности предположить, что критическая неисправность произойдет в самый загруженный момент, когда единственный специалист, хорошо разбирающийся в системе, окажется недоступен. В такой ситуации наличие четко оформленного плана восстановления позволит быстро и правильно вернуть систему в рабочее состояние.

В плане восстановления должна быть подробно указана вся необходимая информация для восстановления критически важных для предприятия систем:

1. лица, ответственные за восстановление системы, с указанием их контактных данных;
2. описание оборудования и программного обеспечения: все устройства, инструменты, данные и версии ПО, необходимые для восстановления, а также их точное местоположение;
3. пошаговая инструкция – какие действия и в каком порядке нужно выполнить;
4. настройки восстанавливаемой системы;
5. учетные данные, необходимые для восстановления (служебные учетные записи, пароли администратора и т. п.).

В случае киберинцидента документы, хранящиеся на сервере, могут оказаться недоступными, поэтому план восстановления следует хранить еще и в распечатанном виде, в заранее определенном и безопасном месте.

7.3 Обеспечьте контроль над тем, что происходит в системах

Помимо защиты IT-инфраструктуры, организация должна иметь четкое представление о том, что происходит внутри систем. Это помогает быстрее обнаруживать атаки и понимать, каким образом злоумышленнику удалось получить доступ.

Для этого необходимо настроить логирование и регулярно отслеживать собранные журналы событий. Важно, чтобы в логах фиксировалась вся критически важная информация – например, данные о сетевом трафике, работе средств защиты, контроллерах домена, серверах (включая административные действия), рабочих станциях и приложениях. Журналы следует хранить не менее одного года, а желательно – до трех лет. Это необходимо для того, чтобы в случае инцидента можно было точно определить, когда началась подозрительная активность и какие системы были затронуты. Ведь злоумышленник может находиться в сети задолго до того, как проявит себя.

Журналы событий следует хранить на отдельном сервере и регулярно создавать их резервные копии, чтобы не потерять данные даже в случае компрометации основной системы. Также рекомендуется внедрить систему мониторинга, которая будет отслеживать работу инфраструктуры и выявлять инциденты безопасности, автоматически уведомляя ответственных лиц при возникновении угроз.

7.4 Обеспечьте работу системы резервного копирования и контроль за ней

При планировании резервного копирования первым делом нужно определить, какие данные являются критически важными для предприятия и подлежат обязательному сохранению. В список таких данных входят электронная почта, базы бизнес-приложений, общие каталоги и файлы, а также информация, хранящаяся на компьютерах сотрудников. Необходимо также включить в резервное копирование технические данные, необходимые для восстановления систем, – например, файлы конфигурации серверов и сетевого оборудования.

Следующий важный шаг – определить, за какой период должна сохраняться возможность восстановления данных. К примеру, критически важные данные, такие как общие папки или база финансовой системы, рекомендуется сохранять ежедневно и хранить копии как минимум за последний месяц – это обеспечит возможность

восстановления информации за 30 дней. Данные, которые редко изменяются (например, фотобанк или архив), можно резервировать раз в месяц и хранить от них только одну актуальную копию.

Посоветуйтесь с IT-специалистом

Обратитесь к своему IT-специалисту или поставщику услуг для организации резервного копирования (какие данные, частота, количество резервных копий).

Чтобы защитить резервную копию в случае несчастного случая (пожара, наводнения) или кражи, следует также создать внешнюю резервную копию. Эта резервная копия может находиться в облаке, в другом офисе или, например, у хостинг-провайдера. Кроме того, одну из резервных копий следует хранить на носителе, не подключенном к сети. Если используется облачный сервис или сторонний провайдер, важно учитывать, что данные будут находиться у третьего лица, и заранее взвесить, стоит ли размещать там конфиденциальную информацию и коммерческие тайны.

Не менее важно убедиться, что резервное копирование действительно работает, – при неудачной или повреждённой копии восстановление данных будет невозможно. Для этого необходимо настроить уведомления на электронную почту о результатах резервного копирования и регулярно проверять журналы выполнения задач, чтобы убедиться, что копии создаются без ошибок. Периодически стоит проверять, все ли нужные данные включены в резервное копирование – например, папка могла быть перемещена, но в настройках резервного копирования это не учтено. При необходимости параметры копирования нужно скорректировать. Также важно вести документацию по резервному копированию: какие данные и куда сохраняются, сколько версий хранится, какая программа используется и другую техническую информацию.

7.5 Проводите тестовые восстановления

Очень важно регулярно выполнять пробное восстановление данных. В рамках такой проверки восстанавливается часть критически важной системы в отдельную среду, чтобы не повлиять на рабочую, – и оценивается, правильно ли всё работает после восстановления. Тестовые восстановления необходимы, потому что даже если кажется, что резервные копии созданы успешно, в процессе восстановления могут возникнуть ошибки, которые невозможно было предугадать. Например, копия может оказаться поврежденной, часть данных – отсутствовать, или выяснится, что для запуска системы требуются дополнительные настройки. Все выявленные отклонения и нестандартные настройки необходимо зафиксировать в плане восстановления. Пробное восстановление нужно проводить для всех критически важных систем, выбирая резервные копии для проверки выборочно.

Посоветуйтесь с IT-специалистом

Узнайте у своего IT-специалиста или поставщика услуг, есть ли у них план по восстановлению данных при несчастном случае, и проводились ли тестовые восстановления, чтобы убедиться, что план работает? При необходимости следует разработать план восстановления и провести пробное восстановление.

8 Защитите свой бренд

С брендом предприятия напрямую связаны его публичные ресурсы – сайты, аккаунты в соцсетях и адреса электронной почты. Поскольку они находятся в открытом доступе, существует риск того, что злоумышленники попытаются их использовать – чтобы навредить репутации предприятия, получить финансовую выгоду или преследовать иные цели. Именно поэтому важно обеспечить их защиту.

8.1 Осознайте возможные угрозы

Публичные сервисы, такие как веб-сайты и электронная почта, подвержены рискам, которые могут нарушить работу предприятия и нанести вред его репутации.

Вот какие угрозы могут возникнуть в случае с веб-сайтами:

1. Злоумышленники могут сделать сайт предприятия недоступным. Это, например, парализует работу предприятия, занимающегося электронной коммерцией, а также помешает работе многих других предприятий, поскольку клиенты смогут не получать необходимую им информацию с вебсайта.
2. Злоумышленники могут взломать административный доступ к сайту и украсть, к примеру, клиентские данные, что повлечет за собой потери в плане репутации и риск получения штрафов за нарушение требований GDPR.
3. Они могут изменить содержимое сайта, разместив на нем неприемлемую (например, оскорбительную) информацию, что также нарушит работу предприятия и подорвет доверие к ней.
4. На сайт может быть установлено вредоносное ПО, заражающее устройства посетителей. Это может привести к тому, что клиенты начнут избегать сайт предприятия, даже если он уже был восстановлен и очищен.

Полезно знать!

GDPR (Общий регламент по защите данных, англ. *General Data Protection Regulation*) – это общеевропейское законодательство, устанавливающее правила обработки персональных данных в пределах Европейского союза. Нарушение положений GDPR может повлечь за собой серьезные штрафы: до 20 миллионов евро или 4% от годового оборота за предыдущий финансовый год, в зависимости от того, какая сумма выше. Такие санкции могут быть применены, если, например, организация проигнорировала внедрение необходимых технических или организационных мер безопасности. Подробнее об этом можно прочитать здесь: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_et.

Если злоумышленники получают контроль над аккаунтами предприятия в социальных сетях, это может нанести урон репутации (например, публикации неподобающего контента, оскорбления клиентов и т. п.), так и к финансовым потерям. Особенно если к этим аккаунтам привязаны платежные данные, такие как информация о кредитной карте для оплаты рекламы в Facebook. Следует учитывать, что помимо корпоративных аккаунтов необходимо защищать учетные записи руководства и ключевых сотрудников предприятия.

Если почтовый сервис предприятия не защищен, злоумышленники могут использовать корпоративные адреса для мошенничества – например, чтобы выманить деньги у сотрудников или партнеров, либо для рассылки спама. Кроме того, письма, отправленные с незащищенного домена, могут блокироваться антиспам-системами почтовых серверов и не доходить до получателей, что также может повлечь за собой потери как для репутации, так и ущерб в финансовом плане.

8.2 Защитите себя от угроз

Первый шаг к защите от угроз – осознание того, что они действительно существуют. Существует целый ряд мер, которые предприятие может предпринять самостоятельно, чтобы предотвратить возможные риски.

8.2.1 Выберите инструменты для выявления уязвимостей

Для атаки на общедоступную службу (например, веб-сайт или почтовый сервер) обычно используются уязвимости в программном обеспечении, слабые настройки безопасности, слишком простые или ранее скомпрометированные пароли и т. п. Существуют инструменты для обнаружения уязвимостей, которые делают это автоматически. Такие инструменты сканируют публичные сервисы и формируют наглядные отчеты об обнаруженных уязвимостях. После обнаружения они должны быть удалены ИТ-персоналом или поставщиком услуг. Затем следует провести повторное сканирование, чтобы убедиться, устранены ли ранее выявленные уязвимости. Такие проверки нужно выполнять регулярно (например, раз в месяц), чтобы своевременно обнаруживать новые уязвимости и устранять их.

Посоветуйтесь с IT-специалистом

Для выявления уязвимостей доступно множество различных решений. Узнайте у своего IT-персонала или поставщика услуг соответствующее программное обеспечение.

8.2.2 Защитите свои публичные сервисы

Чтобы защитить публичные сервисы, необходимо устранить выявленные уязвимости. Особое внимание следует уделить своевременному обновлению программного обеспечения, которое используется для веб-сайтов и почтовых серверов (см. раздел 4.2 «Регулярно обновляйте программное обеспечение»). Обновлять следует как программное обеспечение самого сервера, так и ПО, на котором работает сервис.

Для защиты домена важно убедиться, что контактные данные администратора в доменном реестре указаны правильно. CERT-ЕЕ ведет мониторинг зоны .ee и рассылает уведомления владельцам сайтов, на которых выявлены критические уязвимости или следы компрометации. Актуальные контактные данные позволяют получить такие уведомления вовремя.

Посоветуйтесь с IT-специалистом

Если сервер размещен у провайдера и находится под его управлением, уточните у поставщика услуг, проводится ли регулярное обновление серверного ПО и когда оно выполнялось в последний раз.

Для защиты службы электронной почты ваш IT-персонал или поставщик услуг должен установить следующие параметры:

1. Для защиты почтового трафика серверов необходимо включить поддержку TLS для протокола SMTP, использовать протоколы POP3S и IMAPS, а также отключить на стороне сервера поддержку нешифрованных POP3 и IMAP-соединений. Очень важно, чтобы почтовый сервер использовал только надежные сертификаты, выданные на корректное полное доменное имя сервера (FQDN, *fully qualified domain name*) и с указанием разрешения на использование сертификата для защиты электронной почты (*Email protection*).
2. Чтобы злоумышленники не могли свободно отправлять письма с корпоративных адресов, необходимо создать в DNS SPF-запись (*Sender Policy Framework*) – она указывает, какие почтовые серверы имеют право отправлять письма от имени домена предприятия. Если используются массовые рассылки (например, через Smaily, MailChimp и другие сервисы), их не следует добавлять напрямую в SPF-запись. Вместо этого нужно настроить DKIM, иначе может возникнуть ситуация, при которой любой пользователь того же сервиса сможет отправлять письма от имени вашего домена.
3. Для подтверждения подлинности корпоративного почтового сервера рекомендуется настроить DKIM (*DomainKeys Identified Mail*). DKIM подписывает исходящие электронные письма с сервера, а другие почтовые серверы проверяют правильность подписи.
4. DMARC (*Domain-based Message Authentication, Reporting and Conformance*) – это механизм, который распространяется через DNS и сообщает почтовым серверам,

какие проверки следует применять к письмам, отправленным с данного домена, и как с ними следует поступать. DMARC использует SPF и DKIM для проверки соответствия заданной политике. С его помощью можно получать отчеты о попытках отправки писем от имени вашего домена с неразрешенных серверов.

Полезные рекомендации по защите электронной почты можно найти также в [блоре](#) RIA.³

8.2.3 Защитите свои аккаунты в социальных сетях

Часто атаки направлены на аккаунты предприятия в соцсетях, таких как X (Twitter), LinkedIn, Facebook, Instagram и др. В зоне риска находятся также аккаунты руководителей и ключевых сотрудников, и их следует защищать с не меньшим вниманием.

Для защиты аккаунтов предприятия в социальных сетях следует предпринять ряд простых и недорогих шагов, которые значительно повысят безопасность.

1. Разработайте внутренний регламент использования социальных сетей. В этом документе должны быть указаны:
 - какие соцсети, аккаунты и страницы использует организация и с какой целью;
 - какие сотрудники имеют доступ к каким аккаунтам и в каком объеме;
 - как организован резервный доступ к аккаунтам;
 - как передаются доступы при смене обязанностей или увольнении сотрудника;
 - как сотрудник должен вести себя в социальных сетях.
2. Используйте надежные пароли и меняйте их, если сотрудник, имевший доступ, покидает предприятие.
3. Включите многофакторную аутентификацию.
4. Регулярно проверяйте все корпоративные аккаунты в соцсетях. Сразу же удаляйте доступ у сотрудников, которым он больше не требуется.
5. Периодически пересматривайте настройки аккаунтов. Время от времени платформы могут менять параметры конфиденциальности или сбрасывать их.
6. Даже если аккаунт не используется активно, его нужно защищать и отслеживать так же, как и рабочие – чтобы вовремя выявить попытку захвата.
7. Если вы используете стороннего подрядчика для управления соцсетями, заранее договоритесь, что право собственности на аккаунт и его содержимое остается за компанией.

³ <https://www.ria.ee/blogi/taga-oma-organisatsiooni-e-kirjavahetuse-usaldusvaarsus-ja-turvalisus>

Посоветуйтесь с IT-специалистом

Если предприятие активно присутствует в социальных сетях, стоит рассмотреть возможность использования специального программного обеспечения для защиты аккаунтов. Оно может автоматически удалять подозрительный контент, блокировать публикации несанкционированного характера, отслеживать попытки создания поддельных аккаунтов от имени фирмы и многое другое. Спросите у своего IT-специалиста или поставщика услуг о таких решениях.

9 Обратите внимание на безопасность цепочки поставок

Представьте, что одну и ту же IT-систему одновременно используют юридическая фирма, торговая сеть и строительная фирма. Вместо того чтобы атаковать каждую организацию по отдельности, злоумышленнику проще взломать общую систему – и получить доступ ко всем через нее. Такой тип атаки называется атакой на цепочку поставок.

Подобные атаки могут парализовать работу систем, привести к повреждению или утечке данных и нанести серьезный урон репутации. Нередко они сопровождаются значительными финансовыми потерями.

Если вы используете программное или аппаратное обеспечение сторонних поставщиков, важно понимать: вместе с ним вы принимаете и риски, связанные с их безопасностью.

Чтобы минимизировать эти риски, следует:

1. проверить, проходил ли поставщик аудиты по информационной безопасности и охватывают ли они критически важные для вашей организации аспекты;
2. заключить договор, в котором четко прописаны положения о хранении логов, мониторинге сетей, управлении правами доступа и сегментации сетевой инфраструктуры;
3. установить конкретные требования по безопасности к продуктам и услугам и включить их в договор;
4. определить ответственных лиц с обеих сторон и согласовать каналы связи на случай проблем;
5. заранее договориться о действиях в случае перебоев в предоставлении услуг или инцидентов безопасности;
6. регулярно запрашивать у поставщика отчеты о состоянии систем и результатах их мониторинга.

Помните!

Регулярно проверяйте, соблюдает ли поставщик прописанные в договоре требования по кибербезопасности, и уточняйте, как он реагирует на инциденты, управляет уязвимостями, устанавливает обновления и выполняет свои обязательства.

Особое внимание следует уделить управлению рисками, связанными с безопасностью цепочки поставок. Важно вести документацию по всем поставщикам и фиксировать потенциальные угрозы, связанные с использованием стороннего ПО и оборудования. Для снижения рисков рекомендуется ознакомиться с разделом по управлению рисками Эстонского стандарта информационной безопасности (E-ITS), а также с более широкими рекомендациями по его внедрению.⁴

⁴ <https://eits.ria.ee/>