**КИБЕРБЕЗОПАСНОСТЬ В ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЯХ**

**Харченко Алексей Николаевич, государственное бюджетное профессиональное образовательное учреждение Ростовской области «Шахтинский педагогический колледж», преподаватель,** **Российская Федерация, г. Шахты**

**Аннотация**: Кибербезопасность является растущей проблемой для образовательных учреждений по всем направлениям. Хотя многие люди могут подумать, что угрозы безопасности представляют собой риск только для онлайн-университетов и институтов, правда в том, что они нацелены на всех. Будь то местная начальная школа, государственный университет или портал онлайн-обучения, киберугрозы могут нанести серьезный ущерб.

**Ключевые слова:** кибербезопасность, утечка данных, ресурсы, взлом, киберугрозы, кибермир, кибератака.

Кибербезопасность претерпела много достижений за последнее десятилетие. Благодаря более безопасным способам хранения и обмена информацией мы движемся в правильном направлении.

Однако недостаточно просто обучать учителей, учащихся и лиц, принимающих решения, угрозам кибербезопасности. Должны быть действенные процессы и стратегии, чтобы каждый мог оставаться в безопасности в Интернете.

Мы углубимся в то, как учреждения должны выходить за рамки обучения по вопросам безопасности для обеспечения безопасности организации. Мы расскажем о том, что нужно предпринять, и о том, как смягчить наиболее распространенные киберугрозы, с которыми сталкиваются образовательные учреждения.

**Цель исследования:** определить роль культуры кибербезопасности в защите обучающихся образовательных учреждений от угроз в киберпространстве и наметить направления деятельности по ее формированию в ходе образовательного процесса.

**Что такое кибербезопасность?**

Кибербезопасность — это то, как обеспечить безопасность конфиденциальных данных в цифровой среде. Образовательные учреждения будут иметь много разных областей, которые должны будут обеспечить конфиденциальность и конфиденциальность, когда речь идет о такой информации, как [2, с.30]:

* Частная контактная информация студентов и преподавателей
* Финансовая информация и онлайн-счета, которые могут использоваться учреждением
* Внутренние операционные данные/процессы, которые являются строго конфиденциальными и частными для этого учреждения
* Другие данные, используемые для управления учебными материалами (особенно с точки зрения заданий, экзаменов и оценок).

В дополнение к этим более специфичным для учреждения областям, личные данные также могут быть подвержены риску. Если какие-либо личные учетные записи используются в Интернете учащимися/преподавателями на устройствах учреждения, они также могут быть использованы злоумышленниками.

**Что такое осведомленность о кибербезопасности?**

Осведомленность о кибербезопасности — это степень, в которой потенциально затронутые стороны (учащиеся, сотрудники и лица, принимающие решения) осознают риски для своей информации и конфиденциальности. Образование повышает осведомленность, поэтому люди должны знать, каковы риски, и понимать, какие типы атак и взломов могут произойти [1, с.12].

Однако время от времени проводить обучение по вопросам безопасности — это только первый шаг к продвижению кибербезопасности в образовании. Для обеспечения эффективной безопасности учреждение должно иметь планы на случай инцидентов и гарантировать, что каждый член организации серьезно относится к кибербезопасности.

Ключевые шаги, которые могут вывести осведомленность о безопасности на новый уровень:

* Оценка рисков и информирование о них всех сторон
* Обучение каждого человека, чтобы он понимал, какова его ключевая роль в обеспечении безопасности.
* Получение необходимых ресурсов (и совместное использование ресурсов) внутри учреждений (антивирусное программное обеспечение, доступ к VPN и т. д.)
* Проверка/обновление мер безопасности
* Создание планов реагирования на инциденты.

В этой статье мы рассмотрим каждый из них более подробно.

**Угрозы кибербезопасности в образовании**

Основные угрозы деятельности образовательного учреждения для [безопасности данных](https://tecuy.com/what-is-data-security-types-challenges-and-solutions/184/) следующие:

**Взлом.** Несанкционированный доступ к компьютерной системе/сети, приводящий к краже конфиденциальной информации или повреждению систем. Например, хакеры могут проникнуть в университетскую базу данных и украсть личную информацию сотрудников, а затем получить доступ к их личным финансовым счетам для кражи средств.

**Фишинг.** Злоумышленники используют электронную почту, поддельные веб-сайты или даже текстовые сообщения, чтобы обманом заставить людей раскрыть конфиденциальную информацию, такую ​​как пароли или номера кредитных карт. Поддельные платежные ссылки или счета-фактуры являются одной из наиболее распространенных фишинговых атак, используемых в отношении предприятий и учебных заведений.

**Утечки данных.** Кража, использование или раскрытие конфиденциальной информации (например, личных/финансовых данных).

**Вредоносные программы.** Вредоносное программное обеспечение, наносящее ущерб сети или системе учреждения. К ним относятся трояны, вирусы и программы-вымогатели, которые повреждают устройства, делая их непригодными для использования.

**MitM атаки**: это атаки «человек посередине», когда сообщения перехватываются, а информация, которая отправляется между двумя сторонами, модифицируется злоумышленником.

**Проблемы кибербезопасности в образовательных учреждениях**

Когда учреждения знают о потенциальных проблемах реализации мер кибербезопасности, они могут более эффективно планировать, как обойти эти препятствия.

**Ограничения финансирования.** Не все учреждения имеют доступ к ресурсам, позволяющим внедрять инструменты безопасности. Ограниченный бюджет может привести к менее безопасным серверам, порталам и устройствам. В этом случае поиск внешнего финансирования может быть вариантом, который учреждениям следует изучить.

**Технические навыки.** Для обеспечения надежной кибербезопасности требуется высокий уровень знаний. Самостоятельно некоторым учреждениям будет трудно точно знать, как обеспечить безопасность своих систем, поэтому найм специалиста — это правильный путь.

**Управление людьми.** Никто не может нести ответственность ни за кого другого. Ключевые лица, принимающие решения, могут управлять поведением пользователей (например, создавать правила, запрещающие учащимся получать доступ к социальным сетям на устройствах), но отслеживать такое поведение сложно. Людей необходимо поощрять защищать себя и придерживаться политики.

**Киберугрозы.** В конце концов, угрозы становятся более частыми, а злоумышленники становятся более умными. Вот почему так важно быть в курсе потенциальных угроз по мере изменения технологического ландшафта. Знание того, какие новые угрозы появляются в онлайн-сфере, поможет лицам, принимающим решения, лучше подготовить свою среду и предотвратить какой-либо серьезный ущерб.

**Как реализовать осведомленность о кибербезопасности**

Ниже приводится краткое руководство, которое поможет вам обеспечить надежную кибербезопасность вашего учебного заведения, выходящее за рамки простого обучения по вопросам кибербезопасности.

**Оценка риска**

Существует множество способов проведения оценки рисков для кибербезопасности. Привлечение консультанта, который специализируется в этой области, было бы чрезвычайно ценным. Для учреждений, у которых нет такого бюджета, оценка рисков должна включать исследование всех областей, которые могут быть уязвимы для эксплуатации [4, с.245].

**Стратегия и обучение**

Учреждения должны составить план обеспечения безопасности на основе потенциальных рисков, выявленных в ходе оценки. Для тех, у кого есть бюджет, чтобы привлечь консультанта по кибербезопасности для создания стратегии, это было бы идеально. Если третья сторона провела оценку рисков, она также может создать план для учреждения. Для тех, у кого нет доступа к консультантам, в стратегии будут указаны:

* Роли и обязанности ключевых лиц, принимающих решения
* Обязанности перед большим сообществом (студенты и сотрудники)
* Как будет выполняться каждый этап плана, когда и кем
* Контактные данные каждого ключевого члена команды
* Ресурсы, которые будут использоваться (инструменты, упомянутые ниже).

Вы также можете просмотреть в Интернете несколько бесплатных шаблонов планов и стратегий кибербезопасности, чтобы лучше понять, как их создавать.

Аспект обучения в основном касается информации и ресурсов, к которым каждый член должен иметь доступ для выполнения плана. Кто будет обучать персонал и как их нужно обучать? Что насчет студентов? Чему их нужно обучать? Вариантами обучения являются онлайн-учебники, очные занятия, а также полноценные встречи и семинары.

**Предоставить ресурсы**

Лица, принимающие решения, должны ссылаться на свою оценку рисков и стратегию, чтобы выбрать, какие ресурсы следует использовать и совместно использовать. Некоторые ресурсы и инструменты требуют только однократной загрузки и оплаты, в то время как другие могут предоставляться по подписке, а некоторые могут быть бесплатными.

Вы также должны принять во внимание тот факт, что персоналу обычно требуются средства безопасности, отличные от тех, которые могут использовать студенты. Все это должно быть подробно описано в плане.

Вот лишь некоторые из мер безопасности, в которые любое образовательное учреждение должно инвестировать, если они еще этого не сделали:

* Антивирусная программа
* Менеджеры паролей и инструменты шифрования
* Аутентификаторы для входа
* VPN для устройств организации, в том числе [VPN для мобильных телефонов](https://cybernews.com/best-vpn/vpn-for-iphone/)

Для младших школьников, которые хотят больше узнать о кибербезопасности и даже продемонстрировать заинтересованность в развитии этого навыка в будущем, киберквесты — это интерактивное онлайн-приложение, предназначенное для обучения кибербезопасности.

**Обновите свои планы безопасности**

Наконец, стратегию безопасности всегда необходимо адаптировать к текущим угрозам и любым инновациям в области кибербезопасности. Если новая технология может заменить другие, обновите свои меры и переобучите людей, которым необходимо использовать эту технологию. План никогда не должен стоять на месте, его следует регулярно пересматривать и корректировать. В конце концов, когда дело доходит до кибермира, все меняется быстро.

Частью создания и обновления вашей стратегии кибербезопасности является наличие качественного плана реагирования на инциденты — подробная процедура, когда происходят атаки. В нем должно быть указано, с кем следует связаться, как и какие меры необходимо предпринять для защиты данных и устранения угрозы [3, с.59].

Образовательные учреждения не застрахованы от киберугроз. Необходимо знать не только об опасностях, но и о том, как их смягчить и справиться с ними, когда они случаются. Осознание заводит вас только до сих пор — затем следует действие.

Инвестиции в технологические инструменты, ресурсы, обучение, стратегии и, в конечном счете, совместная работа в команде могут сделать учреждения непроницаемыми и более уверенными в безопасности их конфиденциальной информации.

**Список цитируемых источников**

1. Абрамова Я. Искусственный интеллект на страже кибербезопасности // Директор информационной службы. 2017. №10. С.12.

2. Шимко М.В. Системы сбора информации в аспекте кибербезопасности // Молодой ученый. 2018. №18 (204). С.28-39.

3. Байтерякова А. Профилактика киберэкстримизма в системе школьного образования // Теория и практика современной науки. 2016. № 11 (17). С. 57-61.

4. Степанова О.А., Диденко Г.А., Шварцкоп О.Н. Методические аспекты формирования готовности обучающихся IT-специальностей педагогического колледжа к противодействию вовлечению в киберэкстремистскую деятельность // Азимут научных исследований: педагогика и психология. 2020. Т. 9. № 3 (32). С. 244-247