АКТУАЛЬНЫЕ ЗАДАЧИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В 2023 ГОДУ

КОНСТАНТИН САМАТОВ

Член Правления Ассоциации руководителей служб информационной безопасности

ЧТО ПРОИСХОДИТ?

Массированные компьютерные атаки на информационную инфраструктуру:

- Отказ в обслуживание сервисов и каналов связи
- Дискредитация репутации
- Фишинг, атаки на сотрудников
- Атаки через подрядчиков

Реализация дополнительных мер по обеспечению информационной безопасности: Указ Президента от 1 мая 2022 г.

Усиление требований к безопасности ПДн и КИИ:

- Изменения в 152-ФЗ «О персональных данных»
- Оборотные штрафы (по принципу GDPR)
- Уголовная ответственность за передачу/разглашение ПДн

КУДА БЕЖАТЬ/ЧТО ДЕЛАТЬ?

Массированные компьютерные атаки на информационную инфраструктуру

Что происходит?	Что делать?
Отказ в обслуживании сервисов и каналов связи	АнтиDDOS (от провайдера)
Дискредитация репутации	Заведение внешних ресурсов за WAF, OSINT
Фишинг, атаки на сотрудников	Повышение осведомленности, антифишинговые тренировки, киберучения
Атаки через подрядчиков	• ответственность на уровне договоров; • мониторинг и подключение через СКДП • Проведение работ только после согласования (по возможности)

КУДА БЕЖАТЬ/ЧТО ДЕЛАТЬ?

Изменения в 152-ФЗ «О персональных данных»

Изменение	Чего касается?	Что делать?
Изменения с 01.03.2023		
Оператор обязан провести оценку вреда в соответствии с требованиями, установленными Роскомнадзором, который может быть причинен субъектам ПДн в случае нарушения 152-ФЗ, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных 152-ФЗ	Оценка вреда, который может быть причинен субъектам ПДн	Готовить акты оценки вреда в соответствии с приказом Роскомнадзора от 27.10.2022 N 178 (01.03.23-01.03.29)
Подтверждение уничтожения ПДн в случаях, предусмотренных ст. 21 152-ФЗ, осуществляется в соответствии с требованиями, установленными Роскомнадзором	Уничтожение ПДн	Скорректировать требования к акту уничтожения в соответствии с приказом Роскомнадзора от 28.10.2022 N 179 (01.03.23-01.03.29)
Оператор, осуществляющий сбор персональных данных с использованием ИТС, обязан опубликовать документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных	Политика оператора в области обработки ПДн	Опубликовать политику на каждой странице сайта, где есть формы сбора персональных данных
– **РКН утверждает перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов ПДн. В перечень включаются государства, являющиеся сторонами Конвенции Совета Европы о защите физических лиц, а также иностранные государства, не являющиеся сторонами Конвенции Совета Европы** – **Оператор до начала осуществления трансграничной передачи обязан уведомить РКН о своем намерении. Уведомление направляется отдельно от уведомления о намерении осуществлять обработку ПДн.** – **Оператор до подачи уведомления обязан получить от органов власти иностранного государства, иностранных физических лиц, иностранных юридических лиц, которым планируется трансграничная передача персональных данных, ряд сведений.** – **РКН может запретить или ограничить трансграничную передачу.**	Трансграничная передача ПДн	Перечень утвержден Приказом Роскомнадзора от 05.08.2022 N 128 (вступает в силу 01.03.23) Уведомить о том, что осуществляете/планируете осуществлять трансграничную передачу Распространяется не на все организации
ПРИКАЗ РКН от 14 ноября 2022 г. № 187 • **Что должное содержаться в уведомлении об инциденты** • **Подается или в форме бумажного документа, или через портал РКН** • **Инциденты, связанные с неправомерной или случайной передачей (предоставлением, распространением, доступом) персональных данных, повлекшие нарушение прав субъектов персональных данных**	Взаимодействие РКН с операторами ПДн в рамках **инцидентов**	Корректировка положения об управлении инцидентами, положения о взаимодействии с государственными/надзорными органами.
Приказ ФСБ России от 13 февраля 2023 года № 77: • **«Обычные» операторы – путем заполнения формы на портале РКН, не позднее 24 часов с момента обнаружения, не позднее 72 часов с момента обнаружения о результатах внутреннего расследования** • **Оператор вправе обратиться за помощью в расследовании в НКЦКИ** • **НКЦКИ может отправлять запросу с уточнениями по инциденту на которые оператор обязан отвечать в течении 24 часов.**	Взаимодействие с ГосСОПКА операторами ПДн в рамках **компьютерных инцидентов**	Корректировка положения об управлении инцидентами, положения о взаимодействии с государственными/надзорными органами. Корректировка документации по КЦ ГосСОПКА

ОСНОВНЫЕ РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РИТЕЙЛЕ

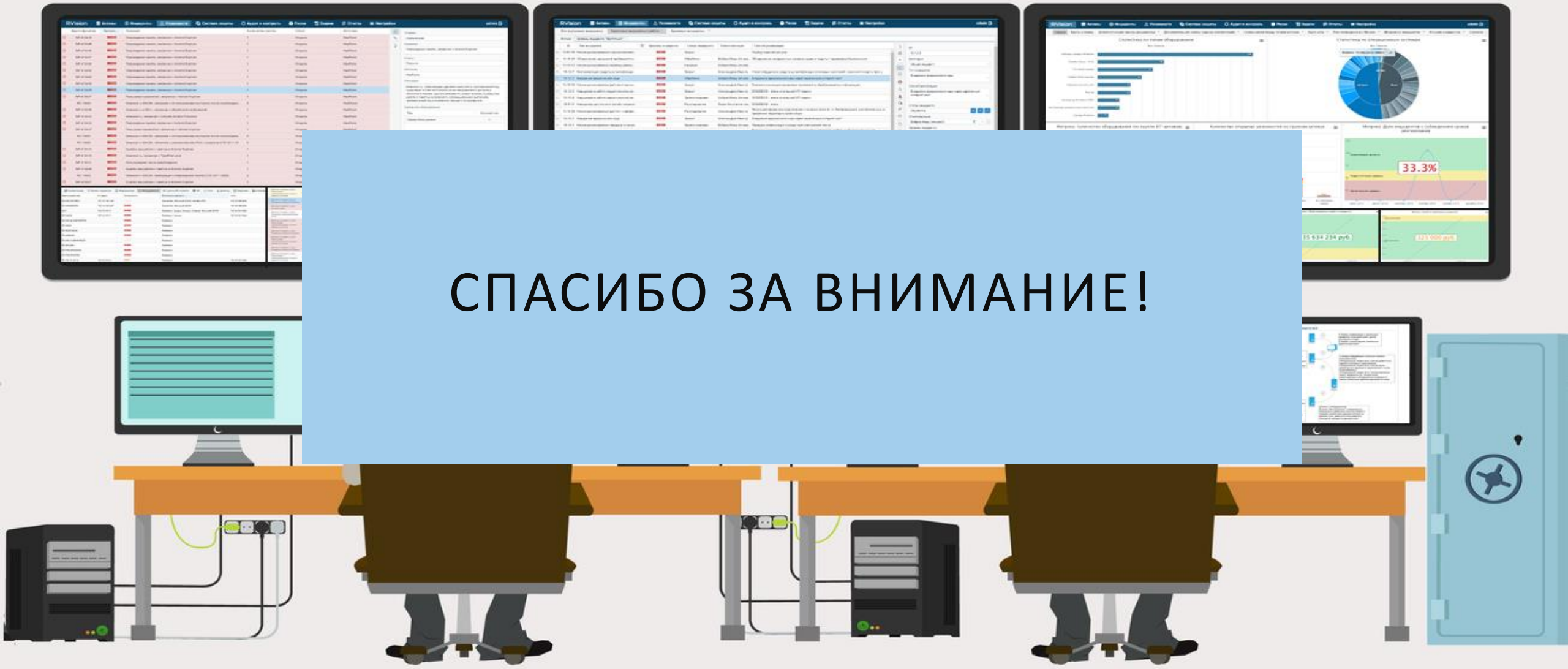
Проводите регулярные аудиты систем безопасности. Это поможет выявить уязвимости в вашей системе и предотвратить возможные кибератаки.

Обучайте своих сотрудников основам информационной безопасности. Они должны понимать, какие действия могут привести к утечке данных или взлому системы.

Используйте двухфакторную (двухэтапную) аутентификацию для доступа внешним ресурсам. Это значительно повысит уровень защиты от несанкционированного доступа.

Храните данные в зашифрованном виде. Это поможет защитить их от кражи или несанкционированного доступа.

Устанавливайте обновления программного обеспечения и антивирусные программы. Это поможет защитить вашу систему от новых угроз.



СПАСИБО ЗА ВНИМАНИЕ!

КОНСТАНТИН САМАТОВ

Член Правления Ассоциации руководителей служб информационной безопасности